

Release Notes

Published
2025-10-03

Junos OS Evolved Release 24.4R2

Introduction

Use these release notes to find new and updated features, software limitations, and open issues for Junos OS Evolved Release 24.4R2.

For more information on this release of Junos OS Evolved, see [Introducing Junos OS Evolved](#).

Table of Contents

Junos OS Evolved Release Notes for ACX Series

What's New | 1

Hardware | 2

Chassis | 32

Interfaces | 32

What's Changed | 33

Known Limitations | 33

Open Issues | 35

Resolved Issues | 37

Junos OS Evolved Release Notes for PTX Series

What's New in 24.4R2-S1 | 41

Interfaces | 41

MACsec | 42

Network Management and Monitoring | 42

Additional Features | 43

What's New in 24.4R2 | 43

Hardware | 44

Chassis | 88

Class of Service | 88

Precision Time Protocol (PTP) | 89

What's Changed | 89

Known Limitations | 90

Open Issues | 92

Resolved Issues | 97

Junos OS Evolved Release Notes for QFX Series

What's New | 102

What's Changed | 102

Known Limitations | 104

Open Issues | 104

Resolved Issues | 106

Upgrade Your Junos OS Evolved Software | 107

Licensing | 108

Finding More Information | 108

Requesting Technical Support | 109

Revision History | 110

Junos OS Evolved Release Notes for ACX Series

IN THIS SECTION

- [What's New | 1](#)
- [What's Changed | 33](#)
- [Known Limitations | 33](#)
- [Open Issues | 35](#)
- [Resolved Issues | 37](#)

These release notes accompany Junos OS Evolved Release 24.4R2 for ACX7020-AC, ACX7020-DC, ACX7024, ACX7024X, ACX7100-32C, ACX7100-48L, ACX7332, ACX7348 and ACX7509 devices. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

What's New

IN THIS SECTION

- [Hardware | 2](#)
- [Chassis | 32](#)
- [Interfaces | 32](#)

Learn about new features introduced in this release for ACX Series routers.

To view features supported on the ACX platforms, view the Feature Explorer using the following links. To see which features were added in Junos OS Evolved Release 24.4R2, click the Group by Release link. You can collapse and expand the list as needed.

- [ACX7024](#)
- [ACX7024X](#)

- [ACX7100-32C](#)
- [ACX7100-48L](#)
- [ACX7332](#)
- [ACX7348](#)
- [ACX7509](#)

The following sections highlight the key features in this release.

Hardware

- **ACX7020 Cloud Metro Router (ACX Series)**—The Juniper Networks ACX7020 Cloud Metro Router is a high-density and temperature-hardened router with a compact 1-U form factor. With 100 Gbps of throughput and advanced timing features, the ACX7020 provides several capabilities that enable you to support mobile backhaul, residential, and metro Ethernet business services solutions.

The ACX7020 features four small form-factor pluggable (SFP28) ports (each configurable as 1GbE, 10GbE, or 25GbE) and sixteen SFP+ ports (each configurable as 1GbE or 10GbE). The router's efficient thermal design allows the use of high-power SFP28 and SFP+ transceivers on all supporting ports.

We ship the ACX7020 routers with integrated fans for side-to-side airflow and built-in AC or DC power supply modules (PSMs).

To install the ACX7020 router and perform initial configuration, routine maintenance, and troubleshooting, see the [ACX7020 Hardware Guide](#). See [Feature Explorer](#) for the complete list of features for any platform.



NOTE: The recommended release for ACX7020 is Junos OS Evolved 24.4R2.

Table 1: ACX7020 Feature Support

Feature	Description
Class of service	<ul style="list-style-type: none"> Support for classification and rewrite rules of all types (Inet-Prec/DSCP/DSCP-v6/IEEE-802.1p/IEEE-802.1ad) at the logical interface level. Supports logical interfaces classification and rewrite rules for MPLS, VPLS, Layer 3 VPN, Layer 2 circuit, CCC, IRB, and EVPN. [See Classifiers and Rewrite Rules at the Global, Physical, and Logical Interface Levels Overview.] <p>NOTE: On IRB interfaces, only Layer 3 classification and rewrite are supported.</p> <ul style="list-style-type: none"> Support for port shaping and scheduling with eight Virtual Output Queues (VOQs) per port and two scheduling priority levels (strict-high and low). Supports multiple strict-high priority queues (RR scheduling), multiple low-priority queues (WFQ scheduling), low latency queues (LLQ), and default deep buffers. [See Schedulers Overview for ACX Series Routers and Shared and Dedicated Buffer Memory Pools on ACX Series Routers .]

Table 1: ACX7020 Feature Support (Continued)

Feature	Description
Dynamic Host Configuration Protocol	<ul style="list-style-type: none"> • DHCP server and DHCP relay configuration for IPv4 and IPv6 services. [See DHCP Overview.] • DHCP relay deployment of EVPN over MPLS, which includes edge-routed bridging (ERB). ERB is an edge model where DHCP clients are connected and relayed in network leaf devices. The spine provider edge (PE) routers do not perform DHCP relay functions. The routers support transit spine functionality, running protocols such as BGP for integrated routing and bridging (IRB). • Support for the following functionalities: <ul style="list-style-type: none"> • EVPN over MPLS Ethernet-LAN • DHCPv4 and DHCPv6 relay options • Stateless forward-only mode for DHCP relay over VPN • Anycast IP address with IRB for a relay source • Client VRFs only • DHCPv4 and DHCPv6 relay agent support for MC-LAG. DHCP relay agent support includes: <ul style="list-style-type: none"> • DHCPv4 and DHCPv6 stateless forward-only option on Layer 3 static interfaces over MC-LAG. • DHCPv4 and DHCPv6 stateless forward-only option on IRB interfaces over MC-LAG. • DHCPv4 and DHCPv6 forward-snooped-clients on dual-stack configurations.

Table 1: ACX7020 Feature Support *(Continued)*

Feature	Description
	<p>[See DHCP Relay Agent and Enabling and Disabling DHCP Snooped Packets Support for DHCP Relay Agent.]</p> <p>[See DHCP Relay Agent in EVPN-MPLS Network.]</p>
EVPN	<ul style="list-style-type: none"> • Support for the following EVPN-MPLS features on MAC-VRF instances: <ul style="list-style-type: none"> • L2 flooding for broadcast, unknown unicast, and multicast (BUM) traffic • Split-horizon between core interfaces • Data plane and control plane MAC learning and aging, and static MAC • MAC movement and MAC mobility on control plane only • MAC limiting and MAC learning • Input and output VLAN maps using normalization on user-to-network interfaces (UNIs) • Aggregated Ethernet interfaces used for UNIs and network node interfaces (NNIs) • Physical interfaces for VLAN tagging, stacked VLAN tagging, flexible VLAN tagging, and extended VLAN bridges using EVPN-MPLS as a service • Ethernet bridge mode for logical UNIs • VLAN ID lists, native VLAN ID-supported logical UNIs, and priority-tagged logical interfaces

Table 1: ACX7020 Feature Support *(Continued)*

Feature	Description
EVPN	<ul style="list-style-type: none"> • Underlay networks with ECMP and fast reroute (FRR) • Control-word support for EVPN • EVPN proxy Address Resolution Protocol (ARP) and ARP suppression • EVPN-ELAN over segment routing [See EVPN Feature Guide.] • NOTE: Data Center feature VXLAN and EVPN-VXLAN is not supported. • Virtual private wire service (VPWS) with EVPN signaling mechanisms and flexible cross-connect support [See Overview of VPWS with EVPN Signaling Mechanisms.] • EVPN E-LAN active/active multihoming with EVPN aliasing support for ESI LAG [See Example: Configuring EVPN Active-Active Multihoming.] • All-active multihoming redundancy in both Ethernet VPN–virtual private wire service (EVPN-VPWS) and EVPN-VPWS with flexible cross-connect [See Overview of Flexible Cross-Connect Support on VPWS with EVPN.] • EVPN VPWS multihoming all-active for segment routing over MPLS [See Overview of VPWS with EVPN Signaling Mechanisms.] • Entropy and flow label for EVPN-ELAN

Table 1: ACX7020 Feature Support *(Continued)*

Feature	Description
	<p data-bbox="898 359 1243 386">[See Configuring Entropy Labels.]</p> <ul data-bbox="862 422 1419 1146" style="list-style-type: none"> <li data-bbox="862 422 1419 449">• Support for the following EVPN-MPLS features: <ul data-bbox="898 485 1419 1146" style="list-style-type: none"> <li data-bbox="898 485 1419 512">• IRB with IPv4 and IPv6 addresses <li data-bbox="898 548 1419 575">• IRB virtual gateway <li data-bbox="898 611 1419 638">• IRB anycast gateway <li data-bbox="898 674 1419 701">• IRB with static MAC <li data-bbox="898 737 1419 806">• EVPN asymmetric Type 2 and symmetric Type 5 routes <li data-bbox="898 842 1419 869">• EVPN E-LAN over BGP-LU <li data-bbox="898 905 1419 974">• EVPN proxy ARP and ARP suppression, and NDP and NDP suppression <li data-bbox="898 1010 1419 1037">• EVPN routing policies <li data-bbox="898 1073 1419 1142">• Ingress virtual machine traffic optimization (VMTO) <p data-bbox="898 1182 1419 1461">[See EVPN with IRB Solution Overview, Anycast Gateways, Symmetric Integrated Routing and Bridging with EVPN Type 2 Routes, Understanding EVPN Pure Type 5 Routes, EVPN Proxy ARP and ARP Suppression, and Proxy NDP and NDP Suppression, Ingress Virtual Machine Traffic Optimization, and Routing policies for EVPN.]</p> <ul data-bbox="862 1497 1419 1724" style="list-style-type: none"> <li data-bbox="862 1497 1419 1524">• Support for the following EVPN-VPWS features: <ul data-bbox="898 1560 1419 1724" style="list-style-type: none"> <li data-bbox="898 1560 1419 1587">• EVPN-VPWS FXC VLAN unaware service <li data-bbox="898 1623 1419 1650">• EVPN-VPWS FXC VLAN aware service <li data-bbox="898 1686 1419 1713">• EVPN-VPWS over segment routing

Table 1: ACX7020 Feature Support *(Continued)*

Feature	Description
	<ul style="list-style-type: none"> • Single homing and all-active multihoming support • Flow-aware transport (FAT) pseudowire labels • Entropy labels <p>[See Overview of VPWS with EVPN Signaling Mechanisms.]</p>
Firewall filters	<ul style="list-style-type: none"> • Support for firewall filters and policers. You can configure firewall filters with packet match conditions for the ethernet switching, IPv4, IPv6, CCC, Any, and MPLS families. In addition to packet match conditions, the ACX7020 supports the count, discard, log, syslog, and policer actions. <p>[See Firewall Filter Match Conditions and Actions in ACX Series Routers (Junos OS Evolved).]</p> <p>NOTE: On IRB interfaces, only Layer 3 classification and rewrite are supported.</p> <ul style="list-style-type: none"> • Filter-based forwarding (FBF). <p>[See Filter-Based Forwarding Overview.]</p> <ul style="list-style-type: none"> • Firewall filter protocols: MPLS, CCC, virtual private LAN service (VPLS), and Any <p>NOTE: On IRB interfaces, only Layer 3 classification and rewrite are supported.</p> <p>[See Firewall Filters Overview, Filter-Based Forwarding Overview, Understanding Filter-Based Forwarding to a Specific Outgoing Interface or Destination IP Address, and Guidelines for gRPC and gNMI Services.]</p>

Table 1: ACX7020 Feature Support *(Continued)*

Feature	Description
High availability	<ul style="list-style-type: none"> • VRRP for IPv4 and IPv6 [See VRRP and VRRP for IPv6 Overview.] • BFD over label-switched paths (LSPs) or RSVP-based LSPs in a centralized mode [See Bidirectional Forwarding Detection (BFD) for MPLS.] • Support for loop-free alternate (LFA) routes for OSPF and IS-IS. LFA enables IP fast-reroute capability for OSPF and IS-IS. [See Loop-Free Alternate Routes for OSPF Overview and Understanding Loop-Free Alternate Routes for IS-IS.] • BFD-triggered fast reroute for unicast next hops. [See Bidirectional Forwarding Detection (BFD) for MPLS, session-id-change-limiter-indirect, and no-bfd-triggered-local-repair.]
Junos telemetry interface (JTI)	<ul style="list-style-type: none"> • Logical subinterface and Packet Forwarding Engine drop, pipe, and line-card counter sensor support for JTI [See Junos YANG Data Model Explorer.]

Table 1: ACX7020 Feature Support *(Continued)*

Feature	Description
Layer 2 features	<ul style="list-style-type: none"> • Ethernet ring protection switching (ERPS) with G.8032 version 2 [See Understanding Ethernet Ring Protection Switching Functionality .] • Support for the following advanced Layer 2 (L2) features: <ul style="list-style-type: none"> • Bridge domain without a <code>vlan-id number</code> statement • Bridge domain with the <code>vlan-id</code> value set to <code>None</code> • Bridge domain with a single VLAN ID • MAC learning, aging, and limiting • Single-learning domain per bridge domain • Ethernet service types: <ul style="list-style-type: none"> • E-Line with these AC interface types: port, VLAN, Q-in-Q, VLAN list, and VLAN maps • E-Line • E-LAN • E-Access • E-Transit • LLDP • LACP • IRB interface

Table 1: ACX7020 Feature Support *(Continued)*

Feature	Description
Layer 2 features	<ul style="list-style-type: none"> • • Link aggregation group (LAG) support with the following hashing algorithms: <ul style="list-style-type: none"> • For family multiservice, destination and source MAC addresses • For family inet, Layer 3 and Layer 4 • For family inet6, Layer 3 destination and source addresses • For family inet6, Layer 4 destination and source ports • Encapsulation types: <ul style="list-style-type: none"> • extended-vlan-bridge • vlan-bridge • ethernet-bridge • Q-in-Q tunneling [See Understanding Layer 2 Bridge Domains and Q-in-Q Tunneling.] • Disable local switching in bridge domains. [See Configuring MAC Address Flooding and Learning for VPLS.] • Layer 2 protocol tunneling (L2PT) to send L2 protocol data units (PDUs) across the network and deliver them to devices that are not part of the local broadcast domain. • Storm control [See Understanding Storm Control.]

Table 1: ACX7020 Feature Support (Continued)

Feature	Description
Layer 2 features	<ul style="list-style-type: none"> • Rapid Spanning Tree Protocol (RSTP), Multiple Spanning Tree Protocol (MSTP), and VLAN Spanning Tree Protocol (VSTP) [See Spanning-Tree Protocol Overview.] • MAC move limit and multiple trunk ports, virtual private LAN service (VPLS), and EVPN networks [See Understanding MAC Limiting and MAC Move Limiting.] • Transparent forwarding of L2CP BPDUs. Layer 2 Control Protocol (L2CP) BPDUs are transparently forwarded in hardware unless a specific protocol is configured on the incoming interface. This feature helps you configure and enable L2PT. • VLAN sensor support [See Telemetry Sensor Explorer.] [See Understanding Layer 2 Bridge Domains on ACX Series and Q-in-Q Tunneling on ACX Series, Bridging and VLANs, and Configuring MAC Address Flooding and Learning for VPLS .] • Multichassis link aggregation groups (MC-LAGs). The following Layer 2 features are available on MC-LAGs: <ul style="list-style-type: none"> • Layer 2 bridging for active/active and active/standby modes • Layer 2 unicast with and without IGMP snooping • Layer 3 unicast with and without IGMP snooping • Layer 2 multicast with and without IGMP or MLD snooping

Table 1: ACX7020 Feature Support (Continued)

Feature	Description
	<ul style="list-style-type: none"> • Layer 3 multicast with and without IGMP or MLD snooping <p>[See Understanding Multichassis Link Aggregation Groups.]</p>
Layer 2 VPN	<ul style="list-style-type: none"> • Support for VPLS. The router supports a single VLAN for each virtual switch routing instance type. Junos OS Evolved does not support the family vpls option. To configure VPLS, configure the instance-type virtual-switch statement at the [edit routing-instances <i>routing-instance-name</i>] hierarchy level. If you configure normalized VLANs, either by not configuring VLAN IDs or by including the vlan-id none statement, then you must include the service-type single statement at the [edit routing-instances <i>routing-instance-name</i> protocol vpls] hierarchy level. <p>[See Introduction to Configuring VPLS.]</p> <ul style="list-style-type: none"> • Support for control word and load-balancing capabilities using entropy and flow-aware transport of pseudowires (FAT) flow labels, across LDP-signaled pseudowires for virtual private LAN service (VPLS) <p>[See control-word , Configuring Entropy Labels, and FAT Flow Labels Overview.]</p> <ul style="list-style-type: none"> • Support for redundant pseudowires for virtual private LAN service (VPLS). The router supports VPLS with LDP hot-standby, cold-standby model, and without BFD or CFM trigger. <p>[See Redundant Pseudowires for Layer 2 Circuits and VPLS.]</p>

Table 1: ACX7020 Feature Support *(Continued)*

Feature	Description
Layer 2 VPN	<ul style="list-style-type: none"> • IRB support for VPLS. [See Configuring VPLS and Integrated Routing and Bridging.] • Layer 2 VPN and L2 circuit support: <ul style="list-style-type: none"> • L2 circuit—Targeted LDP signaling pseudowires and interoperability between different types of supported attachment circuit for L2 circuit • L2 VPN circuit—BGP signaling • MPLS fast reroute (FRR) on IGP, circuit attachment types (port, VLAN, and Q-in-Q tunneling), control word, pseudowire circuit on aggregated Ethernet interfaces, indirect next hops and composite next hops, pipe and uniform mode time-to-live (TTL), Tag Protocol Identifiers (TPIDs), and VLAN map on pop, push, or swap [See Understanding Layer 2 VPNs and Understanding Layer 2 VPNs and Configuring Interfaces for Layer 2 Circuits.] • Flow-aware transport for pseudowires (FAT) label and entropy label support for Layer 2 circuit and Layer 2 VPN [See Configuring Entropy Labels and FAT Flow Labels Overview.]

Table 1: ACX7020 Feature Support *(Continued)*

Feature	Description
Layer 3 features	<ul style="list-style-type: none"> • Support for the following Layer 3 features: <ul style="list-style-type: none"> • IP forwarding and exception packet handling • IEEE 802.1Q (VLAN trunk) on IRB interfaces • Address Resolution Protocol (ARP), neighbor discovery, unicast reverse-path forwarding (unicast RPF), and ECMP • LPM and fragmentation handling, ICMP redirect handling, VLAN tagging modes, neighbor solicitation, and interface-based routing • Longest prefix match • Exception packets handling • VLAN tagging modes • Integrated routing and bridging (IRB) • IPv4 and IPv6 <p>The router also supports interior gateway protocols such as OSPF, IS-IS, RIP, and ECMP for IPv4 and IPv6. [See Configure ICMP Features, Enabling VLAN Tagging, Neighbor solicitation, Understanding Unicast RPF (Routers), OSPF Overview, IS-IS Overview, and RIP User Guide.]</p>

Table 1: ACX7020 Feature Support (Continued)

Feature	Description
Layer 3 VPN	<p>Support for the following Layer 3 VPN features:</p> <p>NOTE: VT interface-based Layer 3 VPN is not supported. Layer 3 VPN ping is supported only with the vrf-table-label configuration.</p> <ul style="list-style-type: none"> • IP-VPN services: <ul style="list-style-type: none"> • Instance-type virtual routing and forwarding (VRF) and virtual router • All control plane configuration options • Per-prefix and per-table label signaling • Layer 3 VPN support with ECMP • BGP policies support for different Layer 3 VPN use cases (for example, full mesh VPN, hub-spoke VPN, management VPN, and leaking routes) • Layer 3 VPN with vrt-table-label mode • Layer 3 VPN with chained composite mode • Import or export of routes across local VRF and global VRF <p>NOTE: Table next hop is not supported.</p> • Inter-autonomous system (inter-AS) options A, B, and C <p>NOTE: You can deploy inter-AS option B can in a hierarchical network design within a single IGP AS.</p>

Table 1: ACX7020 Feature Support *(Continued)*

Feature	Description
	<ul style="list-style-type: none"> • PE to CE routing protocols—Static, eBGP, IS-IS, OSPF, and RIP • IPv6 Provider Edge (6PE)/IPv6 VPN routing over MPLS (6VPE) with PE-CE routing-static and PE-CE BGPv6 <p>[See Layer 3 VPNs User Guide for Routing Devices.]</p>
MPLS	<ul style="list-style-type: none"> • Support for the following MPLS features: <ul style="list-style-type: none"> • IP/MPLS infrastructure feature set for the L3VPN service • Basic BGP control plane features such as LDP-DOD, CSPF, and single-area CSPF • MPLS label stack • MPLS protections: <ul style="list-style-type: none"> • Fast reroute (FRR) and make-before-break (MBB) • Link protection • Node protection • Label-switching router (LSR) • Shared Risk Link Group (SRLG) for MPLS • RSVP label-switched path (LSP) over IPv4 including refresh reduction • Label Distribution Protocol (LDP) LSP over IPv4

Table 1: ACX7020 Feature Support *(Continued)*

Feature	Description
MPLS	<ul style="list-style-type: none"> • RSVP 1:1 • RSVP-Traffic Engineering (RSVP-TE) • LDP over RSVP • Inter-autonomous system LSP intra-area LSP [See MPLS Applications User Guide.] • Support for MPLS LSP statistics and RSVP-TE auto-bandwidth features. Support includes: <ul style="list-style-type: none"> • MPLS LSP statistics for the following LSP types: <ul style="list-style-type: none"> • LDP-signaled LSPs • RSVP-signaled LSPs • Static LSPs • Bypass LSPs • Container LSPs • RSVP-TE auto-bandwidth <p>[See LSP Overview, LDP Overview, RSVP Overview, and Configuring Optimized Auto-bandwidth Adjustments for MPLS LSPs.]</p>

Table 1: ACX7020 Feature Support *(Continued)*

Feature	Description
Multicast	<ul style="list-style-type: none"> • Support for multicast snooping in a VPLS for the following protocols: <ul style="list-style-type: none"> • IGMPv1, IGMPv2, and IGMPv3 snooping in VPLS • MLDv1 and MLDv2 snooping in VPLS • IGMP and MLD snooping in VPLS with integrated routing and bridging (IRB) • Protocol Independent Multicast support over VPLS with IRB <p>[See Multicast Snooping for VPLS.]</p> • Support for Layer 2 multicast-related features, including IGMP and MLD snooping. You can configure IGMP snooping with IGMPv1, IGMPv2, and IGMPv3, which includes support for: <ul style="list-style-type: none"> • IGMP snooping in bridge domains • IGMP snooping with integrated routing and bridging (IRB) configured in bridge domains • MLD snooping in bridge domains • MLD snooping with IRB configured in bridge domains <p>[See IGMP Snooping Overview and Understanding MLD Snooping.]</p> • Support for IPv4 multicast for Layer 3. You can configure IGMP snooping with IGMPv2 and IGMPv3, which includes support for the following: <ul style="list-style-type: none"> • Anycast RP

Table 1: ACX7020 Feature Support *(Continued)*

Feature	Description
	<ul style="list-style-type: none"> • IGMP filter • Protocol Independent Multicast source-specific multicast (PIM SSM) • IGMP querier • PIM sparse mode (PIM SM) <p>[See IGMP Snooping Overview.]</p> <ul style="list-style-type: none"> • Support for BGP MVPN. BGP over MPLS MVPN (also known as "next-generation" MVPN) runs on multipoint LDP provider tunnels, where BGP MVPN is the intra-AS and PIM-SM and multipoint LDP point-to-multipoint (P2MP) tunnels is the data plane. <p>[See Multiprotocol BGP MVPNs Overview.]</p> <ul style="list-style-type: none"> • Multicast with IGMP or MLD snooping within VLANs for EVPN-MPLS <p>[See Overview of Multicast Forwarding with IGMP or MLD Snooping in an EVPN-MPLS Environment.]</p>

Table 1: ACX7020 Feature Support (Continued)

Feature	Description
Network management and monitoring	<ul style="list-style-type: none"> • Support for port mirroring with analyzers and remote port mirroring to IP address (GRE encapsulation) [See Port Mirroring and Analyzers.] • Support for SNMP [See SNMP Architecture and SNMP MIBs Overview.] • Support for Dying Gasp through SNMP in case of power failure. [See Dying Gasp Functionality and SNMP Traps and Informs.]
Operations, Administration, and Maintenance	<ul style="list-style-type: none"> • Support for OAM. You can configure connectivity fault management (CFM), BFD, and the ITU-T Y.1731 standard for Ethernet service OAM. You can also configure the following features of link-fault management (LFM): <ul style="list-style-type: none"> • Discovery • Link monitoring • Remote fault detection [See ITU-T Y.1731 Ethernet Service OAM Overview and Introduction to OAM Link Fault Management (LFM).] • Support for IEEE 802.1ag OAM CFM • Support for IEEE 802.3ah and 802.1ag for OAM CFM down and up maintenance association end points (MEPs) over virtual private LAN service (VPLS)

Table 1: ACX7020 Feature Support (Continued)

Feature	Description
Operations, Administration, and Maintenance	<ul style="list-style-type: none"> Support for IEEE 802.3ah and 802.1ag for OAM CFM up MEPs over EVPN [See IEEE 802.3ah OAM Link-Fault Management Overview and IEEE 802.1ag OAM Connectivity Fault Management Overview.] Support for CFM and performance monitoring (Y.1731) protocols over Ethernet interfaces for bridge and inet services [See Ethernet OAM Connectivity Fault Management.] Support for native Y.1731 operational state sensors to provide statistics such as frame loss ratio, frame delay, frame delay variation, and availability for Y.1731 performance monitoring
Protection against DDoS attacks	<ul style="list-style-type: none"> Support for control plane distributed denial-of-service (DDoS) protection [See Control Plane Distributed Denial-of-Service (DDoS) Protection Overview.]
Routing protocols	<ul style="list-style-type: none"> Layer 3 and routing protocols IPv4, IPv6, BGP, IS-IS, and ARP streaming sensor support using gRPC services Support for unicast reverse path forwarding (unicast RPF): <ul style="list-style-type: none"> Support for loose and strict mode Support for IPv4 and IPv6 [See Understanding Unicast RPF (Routers).]

Table 1: ACX7020 Feature Support *(Continued)*

Feature	Description
Routing protocols	<ul style="list-style-type: none"> • Support for BGP flow specification (BGP flowspec). • The following match conditions are not supported: <ul style="list-style-type: none"> • Fragment for IPv6 • Packet length • Port • Source and destination prefix with offset • The following actions are not supported: <ul style="list-style-type: none"> • Community • Next-term • Routing instance • Sample • Traffic marking <p>[See Understanding BGP Flow Routes for Traffic Filtering.]</p> • Support for configuring interface groups in BGP flowspec filters • BGP Prefix-Independent Convergence (PIC) edge support for inet and MPLS VPNs. The following features are not supported: <ul style="list-style-type: none"> • Session-based repair <p>[See Understanding BGP Flow Routes for Traffic Filtering and Configuring BGP Flow Specification Action Redirect to IP to Filter DDoS Traffic.]</p>

Table 1: ACX7020 Feature Support *(Continued)*

Feature	Description
	<ul style="list-style-type: none"> • BGP PIC over LDP over RSVP tunnel • BGP PIC over SR-MPLS • BGP PIC with RSVP • BGP-LU with PIC • BGP PIC edge protection for Layer 2 services • Protection with multilink failure <p>[See Configuring BGP PIC Edge for MPLS Layer 3 VPNs and Use Case for BGP PIC for Inet.]</p> <ul style="list-style-type: none"> • Support for entropy label for LDP, RSVP, L3VPN, and BGP-LU <p>[See Entropy label support for BGP Labeled Unicast (BGP-LU) and Configuring Entropy Labels.]</p> <ul style="list-style-type: none"> • Support for BGP transport address family or BGP Classful Transport (BGP-CT) includes: <ul style="list-style-type: none"> • Service mapping over colored transport tunnels (RSVP, IS-IS flexible algorithm) to transport classes and map service routes over an intended transport class. The transport tunnels can span multiple domains (ASs or IGP areas). • Network slicing and interoperability between network domains • IPv6 and segment routing-traffic engineering (SR-TE) color-only support • IPv6 and BGP service routes with a color-only mapping community

Table 1: ACX7020 Feature Support (Continued)

Feature	Description
	<ul style="list-style-type: none"> Enhanced transport-class configuration to provide precise resolution <p>[See use-transport-class.]</p>
Services Applications	<ul style="list-style-type: none"> RFC 2544-based benchmarking tests. Support for Layer 2 reflection (bridge, Layer 2 circuit, L2VPN, EVPN-VPWS, EVPN-FXC, EVPN-MPLS, and VPLS), with family ccc or family ethernet-switching and for Layer 3 reflection (IPv4, L3VPN) with family inet. You perform RFC 2544 tests to measure and demonstrate the service-level agreement (SLA) parameters before activation of the service. The tests measure throughput, latency, frame loss rate, and back-to-back frames. <p>[See RFC 2544-Based Benchmarking Tests for ACX Routers Overview.]</p> <ul style="list-style-type: none"> RFC 5357 Two-Way Active Measurement Protocol (TWAMP) monitoring service. You can configure the TWAMP monitoring service, which sends out probes to measure network performance. TWAMP is often used to check compliance with service-level agreements. The support for this service is limited to the following features: <ul style="list-style-type: none"> IPv4 and IPv6 source and target addresses for clients, control connections, and test sessions Probe statistics and history Control and test session status Test session probe generation and reception, as well as reflection

Table 1: ACX7020 Feature Support *(Continued)*

Feature	Description
Services Applications	<ul style="list-style-type: none"> • Timestamps set by software (the Routing Engine or the Packet Forwarding Engine) or hardware • Error reporting through system log messages only • Unauthenticated mode only • Support for sFlow monitoring (ingress) <p>[See sFlow Monitoring Technology and Understanding How to Use sFlow Technology for Network Monitoring.]</p>
Source Packet Routing in Networking (SPRING) or segment routing	<ul style="list-style-type: none"> • Support for the following segment routing features: <ul style="list-style-type: none"> • Segment routing global block (SRGB) for OSPF, IS-IS, and fast reroute • Metro Ethernet services over segment routing infrastructure

Table 1: ACX7020 Feature Support *(Continued)*

Feature	Description
Source Packet Routing in Networking (SPRING) or segment routing	<ul style="list-style-type: none"> • Segment routing services: L3VPN, IPv6 VPN Provider Edge (6VPE) , IPv6 Provider Edge (6PE), L2VPN, L2 circuit, and BGP-VPLS • Static segment routing (node segment, prefix segment, adjacency, and anycast segments) for OSPF and IS-IS • Topology Independent Loop-Free Alternate (TI-LFA) with segment routing for OSPF and IS-IS • Unnumbered interfaces support for segment routing with OSPF • Support for IPv6 L3VPN over IPv6 SR-TE and IPv6 underlay • Support for flexible algorithm in OSPF and IS-IS for segment routing traffic • Interoperability of segment routing with LDP • Support for SRv6 micro-SIDs in IS-IS transport. You can compress multiple SRv6 addresses into a single IPv6 address (micro-SID). For use cases that need to include more than six SRv6 SIDs, micro-SIDs can help in compressing multiple IPv6 addresses. <p>[See How to Enable SRv6 Network Programming in IS-IS Networks.]</p>

Table 1: ACX7020 Feature Support *(Continued)*

Feature	Description
Source Packet Routing in Networking (SPRING) or segment routing	<ul style="list-style-type: none"> Support for BGP link-state distribution with SPRING extensions [See Understanding Topology-Independent Loop-Free Alternate with Segment Routing for IS-IS, Understanding Source Packet Routing in Networking (SPRING), Understanding Adjacency Segments, Anycast Segments, and Configurable SRGB in SPRING, Configure Unnumbered Interfaces, Understanding Static Segment Routing LSP in MPLS Networks, Link-State Distribution Using BGP Overview, Understanding OSPF Flexible Algorithm for Segment Routing How to Configure Flexible Algorithms in IS-IS for Segment Routing Traffic Engineering, and Mapping Client and Server for Segment Routing to LDP Interoperability.] Support for SRv6 network programming in BGP and IS-IS [See Understanding SRv6 Network Programming and Layer 3 Services over SRv6 in BGP and How to Enable SRv6 Network Programming in IS-IS Networks.] Support for SRv6 flexible algorithms in traffic engineering database (TED) and BGP Link State (BGP-LS) [See How to Configure Flexible Algorithms in IS-IS for Segment Routing Traffic Engineering and BGP Link-State Extensions for Source Packet Routing in Networking (SPRING).] SRv6 support for static SR-TE policy. [See Understanding SR-TE Policy for SRv6 Tunnel.]

Table 1: ACX7020 Feature Support *(Continued)*

Feature	Description
Software installation and upgrade	<ul style="list-style-type: none"> • Support for secure-boot implementation based on the UEFI 2.4 standard [See Software Installation and Upgrade Guide.] • Zero-touch provisioning (ZTP) support for WAN interfaces and DHCPv6 options [See Zero Touch Provisioning.]
Timing and synchronization	<ul style="list-style-type: none"> • Support for Synchronous Ethernet over a Link Aggregation Group (LAG). You can define a LAG while configuring the Synchronous Ethernet clock source on these routers. [See Synchronous Ethernet and PTP Overview.] • Support for frequency synchronization using Synchronous Ethernet. [See Synchronous Ethernet Overview.]

Table 1: ACX7020 Feature Support *(Continued)*

Feature	Description
Timing and synchronization	<ul style="list-style-type: none"> • Support for SyncE MIB and PTP MIB. ACX7020 routers support: <ul style="list-style-type: none"> • Defect and event management capabilities for timing features. • SNMP get, get-next, and walk management capabilities for timing features. These capabilities are enabled through the Synchronous Ethernet MIB (SyncE MIB) and Precision Time Protocol MIB (PTP MIB) timing objects. <p>[See Timing Defects and Event Management on Routing Platforms and SNMP MIB for Timing on Routing Platforms.]</p> • Support for G.8275.1 telecom profile, Precision Time Protocol (PTP) over Ethernet encapsulation, and hybrid mode <p>[See Precision Time Protocol Overview and Understanding Hybrid Mode.]</p> • PTP G.8275.1 support over Link Aggregation Group (LAG) <p>[See G.8275.1 Telecom Profile.]</p> • Support for Precision Time Protocol (PTP) G.8275.1 enh and G.8275.2 enh profiles with PTP over IPv4 and IPv6 unicast. The G.8275.1 enh profile does not support unicast negotiation. <p>[See PTP profiles.]</p>

Table 1: ACX7020 Feature Support (Continued)

Feature	Description
Timing and synchronization	<ul style="list-style-type: none"> • Support for PTP G.8275.2 enhanced profile features compliant with the International Telecommunication Union Telecommunication Standardization (ITU-T) G.8273.4 standards. The following key features are supported: <ul style="list-style-type: none"> • Ordinary clocks and boundary clocks • The alternate best timeTransmitter clock algorithm • Full domain and packet-rate ranges • Primary and secondary asymmetry values • Manual mode (no unicast negotiation) and mixed mode • Primary (active) and secondary link configuration. <p>[See PTP Profiles.]</p> • Support for frequency and phase offset relaxation. <p>[See ptp.]</p> • Support for Precision Time Protocol (PTP) Transparent Clock- Regular Transparent Clock (without SyncE) and Syntonised Transparent Clock (with SyncE). <p>[See PTP Transparent Clocks and show ptp global-information.]</p>

- **Supported transceivers, optical interfaces, and DAC cables (ACX7020)**—Select your product in the [Hardware Compatibility Tool](#) to view supported transceivers, optical interfaces, and direct attach copper (DAC) cables for your platform or interface module. We update the HCT and provide the first supported release information when the optic becomes available.

Chassis

- **Chassis management support (ACX7020)**—The ACX7020 router supports these chassis management features:
 - Power Supply Module (PSM) redundancy on ACX7020 with AC power supply
 - Power feed redundancy on ACX7020 with DC power supply
 - Optics Environmental Monitoring (EM) policy for automatic fan speed management
 - Voltage and current monitoring for PSM management

In extremely cold temperatures—for example, at -40°F (-40°C)—the router turns off fans and disables the EM policy. The router restarts operations when the temperature increases to 14°F (-10°C).

We've also made the following CLI command updates:

- `show chassis power` displays combined output for PSM0 and PSM1.
- `show chassis hardware` displays PSMs as built-in.
- `show chassis environment psm` displays PSM state and DC output status.

[See [show chassis power](#), [show chassis hardware](#), [show chassis environment psm](#), and [Optics EM Policy Support](#).]

- **Resiliency support (ACX7020)**—We support resiliency for platform components on ACX7020 routers. Resiliency enables the system to monitor component health, alert you of errors, and take appropriate action to restore normal operation based on error severity.

[See [Resiliency](#).]

Interfaces

- **Support for optical port speeds (ACX7020)**—We support port speeds on optical ports with a default speed set to 10 Gbps. Ensure that total configured port bandwidth does not exceed 100GbE to avoid packet loss. Interface names follow the `et-x/y/z` convention, where *x* and *y* are fixed at 0, and *z* represents the port index. Use the `show chassis pic fpc-slot 0 pic-slot 0` CLI command to check for bandwidth issues and adjust configurations accordingly. Specify unused ports to optimize bandwidth utilization.

[See [Port Speed](#).]

What's Changed

IN THIS SECTION

- [Junos XML API and Scripting](#) | 33

Learn about what changed in this release for ACX Series routers.

Junos XML API and Scripting

- **Refreshing scripts from an HTTPS server requires a certificate (ACX Series and PTX Series)**—When you refresh a local commit, event, op, SNMP, or Juniper Extension Toolkit (JET) script from an HTTPS server, you must specify the certificate (Root CA or self-signed) that the device uses to validate the server's certificate, thus ensuring that the server is authentic. In earlier releases, when you refresh scripts from an HTTPS server, the device does not perform certificate validation. Before you refresh a script using the `set refresh` or `set refresh-from` configuration mode command, first configure the `cert-file` statement under the hierarchy level where you configure the script. The certificate must be in Privacy-Enhanced Mail (PEM) format.

[See [cert-file](#).]

Known Limitations

IN THIS SECTION

- [General Routing](#) | 34
- [Interfaces and Chassis](#) | 34

Learn about limitations in this release for ACX Series routers.

For the most complete and latest information about known Junos OS Evolved defects, use the Juniper Networks online [Junos Problem Report Search](#) application.

General Routing

- When the original flow is egressing out through an aggregated Ethernet (AE) interface, the corresponding sampled sflow frame does not reflect the correct egress port number. This happens only when the flow is egressing out through an AE interface. For non-AE egress interface, this works fine and the sflow frame reflects the correct egress port. [PR1647870](#)
- ACX7024 ports support 10G/1G/25G multi-rate. When peering with other platform or other vendor devices, For example using SFP-LX10 for 1G connection, the link may remain physically down The reason is Auto-negotiation is not supported in ACX7024 PFE due to vendor limitation. In order to make it work, user has to explicitly configure speed/duplex on both sides, and disable auto-negotiation on the peer side. [PR1759804](#)
- With T-GM enabled system like ACX7024, ACX7348 and ACX7332, when primary port link comes up late, then PTP system servo state can move from INITIALIZING to PHASE ALIGNED. This does not cause any issue since when in INITIALIZING state, no PTP packets are sent to down streams devices and in PHASE ALIGNED state, PTP packets are sent with all correct clock parameters. When system moves to directly PHASE_ALIGNED, it is assured that the system is internally locked to phase and frequency of GNSS. [PR1887028](#)

Interfaces and Chassis

- In ACX7020, DIMM used is Non-ECC Unbuffered Memory. Non-ECC (non-parity) unbuffered memory is a type of computer memory that doesn't have an error-detecting feature and is connected directly to the chipset controller. Due to this EDAC driver is not capable to capture ecc related error packets. but these errors can be detected via mcelog. [vrf:none] root@host-pfe-p1c-06:/var/tmp/mce-inject/mce-inject# cd /var/log [vrf:none] root@host-pfe-p1c-06:/var/log# tail -f mcelog.log Tue Nov 12 23:50:38 PST 2024 antman-pfe-p1c-06 mcelog: {"Socket": { "Status": "3 in 24h", "Description": "corrected Socket memory error count exceeded threshold: 3 in 24h", "Total": 3, "Location": "SOCKET:0 CHANNEL:? DIMM:? []", "Socket": 0, "Corrected_Errors": 3, "Uncorrected_Errors": 0, "Time": 1731484236, "Threshold": "0" } } Due to this feature of DIMM , ECC erros cant be captured by EDAC and same cant be refect in cli root@host-pfe-p1c-06> show chassis memory-ecc-statistics Node Name MBE Countt SBE Count SBE Alarm Th Ce Nolnfo Ue Nolnfo SBE Insert SBE Log SBE Alarm re0 0 0 10 Disabled Enabled Enabled <===== though alarm is generated - 2024-11-12 23:50:40 PST Minor Memory corrected error on node Re0[PR1848612](#)

Open Issues

IN THIS SECTION

- [General Routing | 35](#)
- [Interfaces and Chassis | 36](#)
- [Routing Protocols | 36](#)
- [Services Applications | 37](#)

Learn about open issues in this release for ACX Series routers.

For the most complete and latest information about known Junos OS Evolved defects, use the Juniper Networks online [Junos Problem Report Search](#) application.

General Routing

- When DHCP trace options are enabled, there is a possibility that jdhcpd could generate a core file. In general, traceoptions should be enabled only for debugging. They should be disabled once debugging is done. [PR1771121](#)
- Multicast packet duplication occurs under the condition that an ELAN + MVPN network is configured and RP is outside of the core network. In this scenario, egress PE that's non-DF returns multicast traffic to the core side, causing duplication. [PR1820746](#)
- After multiple switchovers **broadsync_lock_failure** alarms are observed on the Junos OS Evolved ACX7348 platform with the PTP (Precision Time Protocol) configured. [PR1826828](#)
- On all ACX Series platforms, all the traffic directed toward an SRv6 (Segment Routing IPv6) dynamic tunnel isn't forwarded inside the tunnel and is dropped. [PR1836457](#)
- On Junos Evolved ACX7100-32C, ACX7332, ACX7348 platforms having ip-demux lite subscriber configured, it is observed that show subscribers interfaces logical ifl-name detail does not display any traffic statistics for ip demux lite subscribers. This is just a display issue and there is no traffic impact due to this issue. [PR1850651](#)
- Storm Control doesn't function when users configure it on an aggregated Ethernet (AE) interface. [PR1852048](#)

- ACX7000 line of Cloud Metro Routers reports an **info-level** log from evo-pfemand tied to remove EcmpNhlnHw textw.[PR1866442](#)
- On Junos Evolved ACX7024 and ACX7024X, the **Active Disk Usage Exceeded** alarm is raised and not cleared even if the usage is less than 50%. This issue has no impact on traffic. [PR1884419](#)
- Under certain conditions, the DHCP registration to the IFL/IFD event fails, and JDHCPD doesn't receive IFL/IFD events. These conditions cause DHCP packets to fail to route to the kernel, resulting in DHCP packet drops. Restarting the DHCP process resolves the issue. Use the CLI command: `restart jdhcpd text`.[PR1884983](#)
- This issue is likely to occur when interfaces are activated, deactivated, created, or deleted. Possible causes for this issue include:
 - A bulk change in interface configuration.
 - An administrator-initiated application restart with the request system application node `re0 restart app application` command.
 - A system-triggered automatic application restart because of internal events.

[PR1885455](#)

Interfaces and Chassis

- If faulty optics or multiple logical interface units are configured, and interfaces flap, the `show interfaces` command might not function. [PR1867451](#)
- Whenever the USB device brand Rally2 is connected to USB port A, a stale `/dev/sda` entry is being created, which results in junk characters being printed in the `show chassis hardware` output. To address this issue a fix has been added to verify whether the opened device is a valid block device. If it's not, the code now skips to the next iteration without processing it. Added logic to sanitize the device string by replacing junk characters with spaces. Introduced additional checks to validate block count and size, preventing further processing of dummy or invalid devices. [PR1890751](#)

Routing Protocols

- The RPD process crashes on Junos OS Evolved platforms in a highly scaled scenario of more than 2000 BGP peers if the BGP sessions are un-configured/brought down abruptly. This leads to loss of routing information and leads to loss of protocol traffic.[PR1756603](#)

Services Applications

- When a device is rebooted with PAA installed in 25.2R1 , PAA installation on reboot might fail due to **Not found default vrf** error. This can be resolved by deactivating and activating or freshly installing the PAA configuration. [PR1886928](#)

Resolved Issues

IN THIS SECTION

- [General Routing | 37](#)
- [Interfaces and Chassis | 40](#)
- [Network Management and Monitoring | 40](#)
- [Routing Policy and Firewall Filters | 40](#)

Learn about the issues fixed in this release for ACX Series routers.

For the most complete and latest information about known Junos OS Evolved defects, use the Juniper Networks online [Junos Problem Report Search](#) application.

General Routing

- Few or all ports on that FPC do not come up after reboot, when one or more port is having an invalid port speed configuration. [PR1738262](#)
- Boot up issue is seen during a software upgrade in ACX7100-32C/ACX7100-48L platforms running Junos OS Evolved. [PR1812515](#)
- Packet corruption in L3VPN traffic with preserve-nexthop-hierarchy. [PR1840722](#)
- ACX7509 : LACP interfaces stuck in attached state. [PR1840790](#)
- High CPU utilization observed on all Junos Evolved ACK7000 platforms. [PR1841573](#)
- Evo-pfemamd process crashes on ACX7348/ACX7332/ACX7024/ACX7509 platforms. [PR1842389](#)

- Junos OS Evolved: ACX7024X - **Exception: [Errno -2] Name or service not known** outputs after issuing `show forwarding-options hash-key`. [PR1846150](#)
- Device does not boot from secondary disk. [PR1846199](#)
- PTP packets which are incoming with padded bytes are dropped on certain Junos OS Evolved ACX platforms. [PR1848586](#)
- Default route installation fails on Junos OS Evolved ACX Series platforms. [PR1848599](#)
- The Devdb messages are seen continuously on ACX Series Junos OS Evolved platforms. [PR1851810](#)
- Firewall policer causing unintended packet drops when VRF route leak with static route to next-table is enabled. [PR1853767](#)
- The IRB VGA is not shown after deleting one of the IRB interfaces with the same VGA address configured. [PR1853879](#)
- The evo-pfemand process crashes on ACX Series platforms without specific trigger. [PR1854255](#)
- ACX Series platform configured as a data center gateway with EVPN-VXLAN failed to forward IP prefix routes for inter-data center communication. [PR1854710](#)
- ACX7100-48L stops working on all LAG members after deactivating one or more interfaces on Junos OS Evolved ACX7000 platforms. [PR1855369](#)
- Random evo-pfemand.re.re0 crash is observed during boot up. [PR1856390](#)
- BFD single hop session flaps seen after a link down event on Junos OS Evolved ACX Series platform. [PR1857248](#)
- Disabling the PIM interface underneath the `edit protocols pim interfaces intf-name` hierarchy might still show PIM as still being UP instead of DOWN. [PR1857699](#)
- Jflow functionality stops working when configured with sflow. [PR1858954](#)
- The firewall filter using **next-ip** as an action does not forward the packets on Junos OS Evolved ACX Series platforms if the **next-ip** is resolved to a static route that points to itself. [PR1859053](#)
- EXP rewrite rules stop working on aggregated Ethernet (AE) interfaces after system reboot. [PR1861541](#)
- The picd process crashes on Junos OS Evolved ACX7509 platforms during Routing Engine switchover. [PR1863708](#)
- Log messages **OOPS: Crossing the LIMIT** are observed on dual Routing Engine platforms. [PR1864880](#)
- The FEC leak is seen on all ACX Series Junos OS Evolved platforms. [PR1865858](#)

- System stops responding to show system applications app ndp detail command or prevents applications from start/stop/restart. [PR1866988](#)
- Packet drops are seen due to stale entries in multicast group when HCoS is enabled on ACX7100 platforms. [PR1867301](#)
- Performance measurement is impacted on deactivating both chassis and PTP configuration and power off USB. [PR1868449](#)
- 100G links do not come up with TX LOS on ACX7100-32C platform. [PR1869296](#)
- The router incorrectly assumes the VRRP primary role on Junos OS Evolved ACX platforms. [PR1869363](#)
- Packet drops are seen for default route when rpf-check loose mode is configured. [PR1869793](#)
- 1G port does not get full bandwidth when ACX7509 device used with Copper SFP and far end device using Intel NIC. [PR1870204](#)
- Interface down is observed while configuring 1G speed on ACX7332/ACX7348/ACX7509 platforms. [PR1870528](#)
- High memory and CPU usage due to unintended phone-home client activation. [PR1871802](#)
- Transient traffic loss during multicast route convergence scenarios. [PR1876781](#)
- Traffic disruption is observed when successive switchover is performed having single-hop BFD configured in the dual Routing Engine scenario. [PR1879925](#)
- The application rpd-agent might restart with a core file after interface related event changes. [PR1885455](#)
- ACX7000 DWDM optics wavelength not applied after reboot. [PR1885817](#)
- VSTP convergence failure on Junos OS Evolved ACX7000 when IRB shares bridge domain with VSTP enabled physical interface. [PR1886421](#)
- Commit can fail if apply-path contains pattern-matching tokens other than the wildcard <*>. [PR1888201](#)
- Matching TOS IP precedence values in the same term by firewall family inet on ACX7100 and all ACX Junos OS Evolved. [PR1891684](#)
- Classification of traffic is not working due to Forwarding Class to Queue mapping configuration failure. [PR1893395](#)
- Auto-negotiation mismatches leading to connectivity issues on Junos OS Evolved ACX7509, ACX7332, and ACX7348 platforms. [PR1893886](#)

- After zeroize, not programmed alarm is seen and SZTP operations might be affected. [PR1899669](#)
- PCIe fatal error resulting in an unexpected device reboot and evo-pfemamd crash on Junos OS Evolved ACX7322 platform. [PR1900115](#)
- ACX7000 logical interface configured with output-traffic-control-profile continues to use physical interface VOQ until ethernet-switching table is cleared. [PR1900224](#)

Interfaces and Chassis

- All the physical links remain down post performing restart **evo-pfemamd** [PR1855426](#)
- Interfaces with the same outer VLAN ID but different inner vlans or inner-lists/ranges report a commit error. [PR1859501](#)
- ACX7024 see's a "\" character in show chassis hardware output. [PR1890751](#)
- Unexpected commit failure is observed when deactivating of unit <unit> or changing any configuration and performing a commit operation. [PR1898055](#)

Network Management and Monitoring

- Configuration under set system trace application app-name gets lost during rollback with certain sequence of steps. [PR1869479](#)

Routing Policy and Firewall Filters

- Routing policy with next hop set to default route 0.0.0.0/0 is not supported. [PR1843116](#)
- When using input-list we do not report the policer stats correctly for Routing Engine filters. This is done correctly for interface-specific filter for the same. [PR1844737](#)
- The firewall process crashes post specific set of filter related modifications performed in single commit. [PR1875725](#)

Junos OS Evolved Release Notes for PTX Series

IN THIS SECTION

- [What's New in 24.4R2-S1 | 41](#)
- [What's New in 24.4R2 | 43](#)
- [What's Changed | 89](#)
- [Known Limitations | 90](#)
- [Open Issues | 92](#)
- [Resolved Issues | 97](#)

These release notes accompany Junos OS Evolved Release 24.4R2 routers. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

What's New in 24.4R2-S1

IN THIS SECTION

- [Interfaces | 41](#)
- [MACsec | 42](#)
- [Network Management and Monitoring | 42](#)
- [Additional Features | 43](#)

Learn about new features introduced in this release for PTX Series routers.

The following sections highlight the key features in this release.

Interfaces

- **Support for 800G Open ZR+ Pluggable Modules (PTX10002-36QDD)**—You can enhance your data center and infrastructure connectivity with high-capacity 800G-ZR+ pluggable modules. These

modules support multiple optical modes and high-performance modulation formats, enabling transmission to reach up to 450 km at 800 Gbps. The optics modules support features such as application selection, wavelength configuration, optical loopback, and configuration of target output power. See [800ZR and 800G OpenZR+ Optical Transceivers](#).

- **Application Selection on 400ZR and 400 G OpenZR+ Optics Modules (PTX10003)**—Application selection allows you to configure different operational modes and optimize performance based on your network needs. You can configure specific applications that define how the optics behaves in terms of reach, capacity, and line system compatibility. You can configure application selection using the set interfaces `<interface> optics-options application hostid <hostid> mediaid <mediaid> [domainid <domainid>]` command under the `interface optics-options` hierarchy. See [Application Selection](#).

MACsec

- **Support for a custom EAPoL EtherType to improve network tunneling of MACsec packets for Layer 2 and Layer 3 traffic (PTX10001-36MR, PTX10002-36QDD, PTX10004, PTX10008, and PTX10016)**—MACsec uses Extensible Authentication Protocol over LAN (EAPoL) as a transport protocol to establish sessions. Some networks filter packets based on their EtherType value. By default, the EtherType for all EAPoL packets is 0x888e. To ensure the network tunnels the MACsec packets properly, you can set a custom EtherType for EAPoL packets.

To configure an EAPoL profile with a custom EtherType, use the `ether-type ether-type-value` statement at the `[edit forwarding-options custom-eapol-ether-type-profiles (EAPOL_ETHERTYPE1 | EAPOL_ETHERTYPE2)]` hierarchy level. By default, the EtherType value for the EAPOL_ETHERTYPE1 profile is 0x876f and the EtherType value for the EAPOL_ETHERTYPE2 profile is 0xb860. If you configure a different value, you must use an EtherType that isn't already reserved for another use. To apply the EtherType to MACsec packets, configure the `eapol-ethertype-profile eapol-profile-name` statement at the `[edit security macsec connectivity-association ca-name mka]` hierarchy level.

[See [Media Access Control Security \(MACsec\) over WAN](#).]

Network Management and Monitoring

- **SNMP support for coherent ZR optics performance monitoring and threshold alerts (PTX10002-36QDD and PTX10003)**—You can monitor the performance of coherent ZR optics (100ZR, 400ZR, 400ZR-M, and 400ZR-M-HP) and receive threshold crossing alerts using SNMP. Retrieve real-time, historical, and statistical data for various performance parameters through SNMP Get requests. You also can receive trap notifications for threshold crossing alerts and clear events.

Use the updated enterprise MIB named Juniper-IFOPTICS-MIB to comprehensively monitor and manage coherent ZR series transceivers.

[See [show snmp mib](#), [Enterprise-Specific MIBs for Junos OS Evolved](#), and [SNMP MIB Explorer](#).]

- **SNMP MIB walk and traps support for coherent ZR optics (PTX10002-36QDD and PTX10003)**—Use SNMP MIB walk and traps to efficiently monitor and manage coherent ZR optics, including 100ZR,

400ZR, 400ZR-M, and 400ZR-M-HP. Use this feature to retrieve OID information sequentially and receive notifications when alarms are triggered or cleared. This enhancement extends SNMP MIB walks to include new digital optical monitoring (DOM) fields and implements SNMP traps for critical alarms.

[See [Enterprise-Specific MIBs for Junos OS Evolved](#) and [show snmp mib](#).]

Additional Features

We've extended support for the following features to these platforms.

- Support for appsel number configuration and display of Q-factor and Q-margin in 400ZR and 400G OpenZR+ optics (PTX10001-36MR, PTX10002-36QDD, PTX10004, PTX10008, and PTX10016)

[See [appselid](#), [optics-options](#), [show interfaces diagnostics optics-applications](#), and [show interfaces diagnostics optics \(Routers\)](#).]

- **Support for performance monitoring and TCA (PTX10002-36QDD)**—We support performance monitoring for the QDD-800G-ZR optical transceiver modules. The current and historical performance monitoring metrics are accumulated into 15-minute and 1-day interval bins. But you can configure the length of the time intervals for 15-minute bins that PM data is accumulated for. You can view the metrics by using the `show interfaces transport pm` command and can manage optical transport link efficiently.
- User configurable PM intervals for more granular and precise network performance monitoring (PTX10001-36MR, PTX10002-36QDD, PTX10003, PTX10004, PTX10008, and PTX10016)

[See [User Configurable PM Interval Length](#), [Configure User Configurable PM Interval Length, interval-length \(Chassis\)](#), [optics \(Chassis\)](#), [Coherent Optics Performance Monitoring](#), and [show interfaces transport pm](#).]

What's New in 24.4R2

IN THIS SECTION

- [Hardware](#) | 44
- [Chassis](#) | 88
- [Class of Service](#) | 88
- [Precision Time Protocol \(PTP\)](#) | 89

Learn about new features introduced in this release for PTX Series routers.

To view features supported on the PTX platforms, view the Feature Explorer using the following links. To see which features were added in Junos OS Evolved Release 24.4R2, click the Group by Release link. You can collapse and expand the list as needed.

- [PTX10001-36MR](#)
- [PTX10002-36QDD](#)
- [PTX10003](#)
- [PTX10004](#)
- [PTX10008](#)
- [PTX10016](#)

The following sections highlight the key features in this release.

Hardware

- **New PTX10K-LC1301-36DD Line Card (PTX10008)**—The PTX10K-LC1301-36DD line card features 36 ports, delivering a line rate throughput of 28.8 Tbps. The 36 high-density 800-Gigabit Ethernet (800 GbE) QSFP-DD ports supports speeds up to 800 Gbps. The line card houses two Juniper Networks' custom Express 5 ASICs, and each ASIC comprises of two Packet Forwarding Engines.

[See [PTX10008 Line Card Components and Descriptions](#).]

- **New JNP10008-SF5 switch interface board (PTX10008)**—The JNP10008-SF5 switch interface board (SIB) supports up to 28.8 Tbps of bandwidth per slot for the PTX10KLC1301-36DD line card installed in PTX10008 router running Junos OS Evolved.

[See [PTX10008 Switch Fabric](#).]

- **Table 2: Features Supported on PTX10K-LC1301-36DD line card for PTX10008 routers**

Feature	Description
Chassis	Packet Forwarding Engine resiliency (PTX10008)— We provide resiliency feature support for Packet Forwarding Engine (PFE) on the PTX10008 device with PTX10K-LC1301-36DD line card. This feature enables the system to detect, report, and take action on PFE faults. Actions are taken based on default configuration or user configuration available for the errors.
	Fabric hardening and resiliency support on PTX10K-LC1301-36DD line cards for PTX10008 devices. [See Fabric Hardening and Recovery on PTX10K Devices .]

Table 2: Features Supported on PTX10K-LC1301-36DD line card for PTX10008 routers (*Continued*)

Feature	Description
	<ul style="list-style-type: none"> • Interoperability support and CLI enhancements (PTX10008)—PTX10008 router with JNP10008-SF5 switch interface board (SIB) supports default interoperability between the PTX10K-LC1301-36DD, PTX10K-LC1201-36CD and PTX10K-LC1202-36MR line cards. Use the <code>set chassis interoperability express5-enhanced</code> command to bring up the system in the <code>express5</code> mode-specific functionalities. This disables the line card interoperability feature. You can verify the interoperability status using the <code>show chassis interoperability</code> command. <p>The existing commands for PTX10008 with PTX10K-LC1201-36CD line card will support for PTX10008 with PTX10K-LC1301-36DD line card as well. Following are the new CLI command updates:</p> <ul style="list-style-type: none"> • The <code>show chassis fpc slot detail</code> command displays PFE ASIC type. • On the <code>set chassis fpc</code> command, you must use <code>pfe-instance</code> instead of <code>pfe</code>. • The <code>show chassis fpc 5 pfe-instance all</code> command displays <code>pfe-instance</code> in the output. <p>[See interoperability, show chassis interoperability, chassis, and show chassis fpc.]</p>

Table 2: Features Supported on PTX10K-LC1301-36DD line card for PTX10008 routers *(Continued)*

Feature	Description
	<ul style="list-style-type: none"> • Fabric resiliency support for JNP10008-SF5 SIB (PTX10008)—The JNP10008-SF5 SIB supports fabric resiliency, enhancing fault management for fabric links. You can benefit from features including error detection, logging, alarm generation, SNMP trap sending, LED error indications, and self-healing. Utilize the CLI command <code>show system errors active detail</code> to view logged errors, ensuring comprehensive fault monitoring and increased system reliability. <p>[See Fabric Resiliency and show system errors active.]</p>
	<ul style="list-style-type: none"> • FPC fabric management for JNP10008-SF5 SIB (PTX10008)—You can use CLI command <code>set chassis fpc</code> to manage FPC online and offline states gracefully. Use the <code>set chassis fabric event reachability-fault</code> command to configure options for detecting fabric reachability faults and trigger automatic connectivity restoration. Additionally, use the extended keyword in <code>show chassis fabric fpcs</code> and <code>show chassis fabric sibs</code> commands to view detailed link information within planes, and identify partially enabled planes with the <code>Degraded</code> keyword in <code>show chassis fabric fpcs</code> command. <p>[See reachability-fault, show chassis fabric fpcs, and show chassis fabric sibs.]</p>

Table 2: Features Supported on PTX10K-LC1301-36DD line card for PTX10008 routers (*Continued*)

Feature	Description
	<ul style="list-style-type: none"> • Support for JNP10008-SF5 SIB (PTX10008)—The PTX10008 supports the JNP10008-SF5 Switch Interface Board (SIB), which includes 18 fabric planes. You can use the extended keyword with the <code>show chassis sibs</code> command to view detailed plane information. Utilize the <code>set chassis sib</code> command to gracefully bring SIBs online or offline. Note that mixing JNP10008-SF3 SIB with JNP10008-SF5 SIB will result in compatibility errors indicated by specific CLI commands: <ul style="list-style-type: none"> • The <code>show chassis sibs detail</code> command displays <code>Incompatible</code> with other SIBs in the output. • The <code>show chassis alarms</code> command displays <code>SIB Incompatible</code> in the output. • The <code>request chassis sib online</code> command displays <code>Request failed since Fru is incompatible with other slots!</code> in the output. <p>[See show chassis sibs, show chassis alarms, request chassis sib, and Fabric Management on PTX10K Devices.]</p> • Optics EM policy support (PTX10008)—The Environment Monitoring (EM) policy now includes optics temperature sensors for PTX10008 routers with PTX10K-LC1301-36DD line card. It ensures efficient thermal management of high-power optical modules. Key functionalities include temperature monitoring integration, automatic shutdown procedures, and CLI commands for managing and configuring the EM policy. <p>[See Optics EM Policy Support.]</p>

Table 2: Features Supported on PTX10K-LC1301-36DD line card for PTX10008 routers *(Continued)*

Feature	Description
Class of Service (CoS)	<p>Support for class-of-service (CoS) features, including classifiers (behavior aggregate (BA), fixed, and multifield (MF)), rewrite rules, forwarding classes, loss priorities, transmission scheduling, rate control, drop profiles, HCoS, and policy map .</p> <p>[See CoS Features and Limitations on PTX Series Routers and Class of Service.]</p>
	<ul style="list-style-type: none"> • Support for on-chip queue buffer for PFC-enabled queues (PTX10008) – A PFC-enabled queue with a buffer-size less than 450 microseconds is viewed and installed as a PFC-enabled on-chip queue. When a queue is in PFC on-chip mode, the entire VOQ buffer is always on-chip and is not scaled based on bandwidth usage. <p>[See buffer-size (Schedulers).]</p>
Dynamic Host Configuration Protocol (DHCP)	<p>DHCPv4 Relay Agent and DHCPv6 Relay Agent are supported. Features included are:</p> <ul style="list-style-type: none"> • DHCP Relay: Layer 3 (L3) interfaces • DHCP Relay: Option 82 for Layer 2 VLANs • DHCP Relay: Option 82 for L3 interfaces • Extended DHCP Relay Agent • Virtual router-aware DHCP (VR-aware DHCP) <p>[See Extended DHCP Relay Agent Overview.]</p>

Table 2: Features Supported on PTX10K-LC1301-36DD line card for PTX10008 routers *(Continued)*

Feature	Description
EVPN	<ul style="list-style-type: none"> • Support for EVPN-VXLAN L2 gateways and L3 gateways with EVPN Type 5 routes. [See EVPN User Guide.] • Support for ping and traceroute for EVPN-VXLAN [See Understanding Overlay ping and traceroute Packet Support.] • Support for Static VXLAN (L2 gateway) [See Static VXLAN.]
	<p>Support for EVPN-MPLS Layer 2 and Layer 3 Features</p> <p>[See EVPN Overview.]</p>
	<p>Support for EVPN-VPWS</p> <p>[See Overview of VPWS with EVPN Signaling Mechanisms.]</p>

Table 2: Features Supported on PTX10K-LC1301-36DD line card for PTX10008 routers *(Continued)*

Feature	Description
Infrastructure	<ul style="list-style-type: none"> • We support the following IP and Infrastructure features: • Junos Telemetry Interface support for Packet Forwarding Engine sensors for usage, network processing unit (NPU) memory, NPU utilization, and pipeline NPU and ASIC. Using the Junostelemetry interface (JTI), you can export statistics using remote procedure call (gRPC) services, gRPC Network Management Interface (gNMI) services, and UDP transport. <p>Use these sensors:</p> <ul style="list-style-type: none"> • <code>/junos/system/linecard/packet/usage/</code> • <code>/junos/system/linecard/npu/memory/</code> • <code>/junos/system/linecard/npu/utilization/</code> • <code>/components/component/integrated-circuit/state/</code> • <code>/components/component/integrated-circuit/pipelinecounters/</code> <p>For pipeline sensors, the four packet and drop counter categories are interface, lookup, queuing, and host interface.</p> <p>[See Junos YANG Data Model Explorer.]</p> <ul style="list-style-type: none"> • Traffic drops classification based on trap classification • Support for DDoS IS-IS classification and higher DDoS bandwidth for Layer 2 and Layer 3 protocols. <p>[See show ddos-protection protocols isis and protocols (DDoS).]</p>

Table 2: Features Supported on PTX10K-LC1301-36DD line card for PTX10008 routers (*Continued*)

Feature	Description
	<ul style="list-style-type: none"> • Support for load balancing under the [edit forwarding-options enhanced-hash-key] hierarchy. Load balancing includes: <ul style="list-style-type: none"> • GRE key inclusion for transit IPv4 and IPv6 traffic • IP Layer 3 fields • IP Layer 4 fields • IPv6 flow label inclusion • MPLS labels • MPLS port data • MPLS pseudowire traffic • Tunnel endpoint identifier (TEID) inclusion in GPRS tunneling protocol (GTP) packets • RSVP-TE load balancing in proportion to LSP bandwidth <p>[See enhanced-hash-key.]</p> <p>Support for 128-way equal-cost multipath (ECMP) routing for MPLS transit cases.</p> <p>The following features do not support 128-way ECMP:</p> <ul style="list-style-type: none"> • Multicast • P2MP • MC-LAG • Weighted unilist

Table 2: Features Supported on PTX10K-LC1301-36DD line card for PTX10008 routers *(Continued)*

Feature	Description
	<ul style="list-style-type: none">• Consistent hashing• Link protection (MPLS)• Adaptive load balancing• Class-based forwarding <ul style="list-style-type: none">• Support for classification override configured under a forwarding policy. [See CoS Features and Limitations on PTX Series Routers and Overriding the Input Classification.]• You can configure passive monitoring on any interface on the PTX10008 routers to monitor MPLS-encapsulated packets. [See Passive Monitoring and passive-monitor-mode.]

Table 2: Features Supported on PTX10K-LC1301-36DD line card for PTX10008 routers (*Continued*)

Feature	Description
Interfaces and Chassis	<ul style="list-style-type: none"> • Support for VRRP. The following features are not supported for VRRP on Junos OS Evolved: <ul style="list-style-type: none"> • ISSU • Proxy ARP • MC-LAG • Distribution support on aggregated Ethernet interfaces • IRB • Inline delegation <p>[See Understanding VRRP.]</p> • Support for the following protocols: <ul style="list-style-type: none"> • LAG (aggregated Ethernet) • LACP • LLDP • Support for link fault management (LFM)—We support IEEE 802.3ah OAM LFM to monitor point-to-point Ethernet links that are connected either directly or through Ethernet repeaters. The following LFM features are supported: <ul style="list-style-type: none"> • Link discovery with active and passive modes • Detect-LOC • Remote loopback • Loopback tracking • Action profile

Table 2: Features Supported on PTX10K-LC1301-36DD line card for PTX10008 routers *(Continued)*

Feature	Description
	<ul style="list-style-type: none"> • GRES and non-graceful Routing Engine switchover <p>[See Introduction to OAM Link Fault Management (LFM).]</p>
	<p>We support the following optics:</p> <ul style="list-style-type: none"> • 800G • 400G • 100G/2x100G • 10GbE/25GbE/40GbE • We support Mac address accounting for 10GE, 40GE, 100GE, 200GE, 400GE, and 800GE interfaces • Support for media access control (MAC) accounting for source and destination macs for Layer 3 interfaces—We support media access control (MAC) accounting for source and destination macs for Layer 3 interfaces and aggregated Ethernet interfaces. To enable MAC accounting, use the existing <code>mac-learn-enable</code> command under the <code>[edit interfaces interface-name gigether-options ethernet-switch-profile]</code> or <code>[edit interfaces aex aggregated-ether-options ethernet-switch-profile]</code> hierarchy level.

Table 2: Features Supported on PTX10K-LC1301-36DD line card for PTX10008 routers *(Continued)*

Feature	Description
IP Tunneling	<ul style="list-style-type: none"> Support for the following PFE tunnel features: <ul style="list-style-type: none"> Filter-based GRE encapsulation and de-encapsulation and filter-based MPLS-in-UDP de-encapsulation. We've enabled the following encapsulation and de-encapsulation workflow: <ol style="list-style-type: none"> An incoming packet matches a filter term with an encapsulate action. The packet is encapsulated in an IP+GRE header and is forwarded to the endpoint's destination. <pre> set firewall tunnel-end-point <i>tunnel-name</i> ipv4 ipv6 source-address <i>address</i> set firewall tunnel-end-point <i>tunnel-name</i> ipv4 ipv6 destination-address <i>address</i> set firewall tunnel-end-point <i>tunnel-name</i> gre set firewall family inet inet6 filter <i>name</i> term <i>name</i> from source-address <i>address</i> set firewall family inet inet6 filter <i>name</i> term <i>name</i> then encapsulate <i>tunnel-name</i> set firewall family inet inet6 filter <i>name</i> term last then accept set interfaces <i>interface-name</i> unit <i>number</i> family inet inet6 filter input set interfaces <i>interface-name</i> unit <i>number</i> family inet inet6 address <i>address</i> # This source address differs from the one for the tunnel endpoint.</pre>

Table 2: Features Supported on PTX10K-LC1301-36DD line card for PTX10008 routers (Continued)

Feature	Description
	<p>2. At the destination, the packet matches a filter term with a de-encapsulate action. The GRE header or MPLS-in-UDP header is stripped from the packet. The inner packet is routed to its destination.</p> <pre> set firewall family inet inet6 filter name term name from source-address address set firewall family inet inet6 filter name term name from protocol gre set firewall family inet inet6 filter name term name then decapsulate gre # Optionally de-encapsulate mpls-in-udp. set firewall family inet inet6 filter name term last then accept set interfaces interface-name unit number family inet inet6 filter input filter-name set interfaces interface-name unit number family inet inet6 address address # This is the destination address. </pre> <p>[See Components of Filter-Based Tunneling Across IPv4 Networks and tunnel-end-point.]</p> <ul style="list-style-type: none"> FTI Tunnels- Support for FTI-based encapsulation and de-encapsulation of IPv4 and IPv6 packets. You can configure IP-IP encapsulation and de-encapsulation on flexible tunnel interfaces (FTIs). The default mode is loopback encap mode. Use the bypass-loopback statement at the [edit interfaces fti number unit logical-unit-number tunnel encapsulation ipip] hierarchy level to change into flattened encap mode to achieve line-rate performance.

Table 2: Features Supported on PTX10K-LC1301-36DD line card for PTX10008 routers *(Continued)*

Feature	Description
	<p data-bbox="932 359 1386 422">[See Tunnel and Encryption Services Interfaces User Guide for Routing Devices.]</p> <ul style="list-style-type: none"> <li data-bbox="898 459 1409 1003">• Support for configuring MPLS protocols over FTI tunnels, thereby transporting MPLS packets over IP networks that do not support MPLS. Generic routing encapsulation (GRE) and UDP tunnels support the MPLS protocol for both IPv4 and IPv6 traffic. You can configure encapsulation and deencapsulation for the GRE and UDP tunnels. To allow the MPLS traffic on the UDP tunnels, include the mpls port-number statement at the [edit forwarding-options tunnels udp port-profile profile-name] hierarchy level. To allow the MPLS traffic on the GRE tunnels, include the mpls statement at the [edit interfaces fti0 unit unit family] hierarchy. <p data-bbox="932 1035 1373 1062">[See Flexible Tunnel Interfaces Overview.]</p> <ul style="list-style-type: none"> <li data-bbox="862 1100 1409 1377">• Egress Filter based encapsulation. For an outgoing packet matching the filter term, the packet is encapsulated inside an IP + GRE header as specified by the tunnel configuration. IP lookup is performed on the outer header and packet is forwarded accordingly. The IP lookup for GRE-encap capable route is limited to the implicit default routing-instance. <p data-bbox="898 1409 1344 1472">[See Understanding Filter-Based Tunneling Across IPv4 Networks.]</p> <ul style="list-style-type: none"> <li data-bbox="862 1509 1409 1612">• Egress Filter routing instance action- Support for configuring output filter action with non-default routing instance or a specified routing instance. <p data-bbox="898 1644 1320 1671">[See Firewall Filter Terminating Actions.]</p> <ul style="list-style-type: none"> <li data-bbox="862 1709 1344 1772">• Ingress Filter based decapsulation by using firewall filters for GRE and UDP tunnels

Table 2: Features Supported on PTX10K-LC1301-36DD line card for PTX10008 routers *(Continued)*

Feature	Description
	[See Configuring a Filter to De-Encapsulate GRE Traffic and decapsulate (Firewall Filter) .]
Junos Telemetry Interface	<p>Junos telemetry interface (JTI) supports new platform sensors for PTX10008. You can export platform-specific software and chassis component statistics using remote procedure call (gRPC) services, gRPC Network Management Interface (gNMI) services, and UDP transport. New xpaths are added in the YANG Data Model. For a complete list of xpaths supported by the device, see Junos YANG Data Model Explorer.</p> <p>[See Junos YANG Data Model Explorer.]</p>

Table 2: Features Supported on PTX10K-LC1301-36DD line card for PTX10008 routers *(Continued)*

Feature	Description
	<p>Packet Forwarding Engine's In-Band Network Telemetry for PTX routers. The Junos EVO Packet Forwarding Engine introduces a framework in the data plane, called In-Band Network Telemetry (INT), which collects and reports network state information, without the intervention of the control plane. The header in the INT model has telemetry instructions that instruct an INT-capable device the state it must collect. The network state information is exported by the data plane either to the telemetry monitoring system or is written into the packet.</p> <p>INT has source, transit and sink support. INT source embeds the INT metadata in the packet and sink collect the metadata from the data packet for processing. We do not support INT source, sink and all INT application modes on PTX10008 routers. Juniper JNP10K-LC1301-36DD line card on PTX10008 supports only INT transit node in Junos OS Evolved Release 24.4R1. Among the three INT application modes INT-XD, INT-MX, and INT-MD, Juniper JNP10K-LC1301 line card on PTX10008 supports only INT-MD mode and INT as a transit node.</p> <p>The set forwarding-options configuration statement is updated with a new inband-telemetry option, to enable or disable this feature.</p> <p>[See Junos YANG Data Model Explorer.]</p>
Layer 2 Features	<p>Support for Q-in-Q tunneling (PTX10008).</p> <p>[See Configuring Q-in-Q Tunneling and VLAN Q-in-Q Tunneling and VLAN Translation.]</p>

Table 2: Features Supported on PTX10K-LC1301-36DD line card for PTX10008 routers *(Continued)*

Feature	Description
	<ul style="list-style-type: none"> • Support for basic Layer 2 features (PTX10008). The PTX10008 router supports the following Layer 2 basic learning, bridging and flooding features: <ul style="list-style-type: none"> • Enterprise-style bridging (support both trunk and access mode) • Service provider-style bridging (also known as sub-interface mode) • BPDU block/filter • xSTP • Handle BUM (broadcast, unknown unicast and multicast) traffic, including split horizon • MAC learning and aging • Static MAC addresses • Trunk port and VLAN membership • 802.1Q EtherType—8100 • 802.1Q VLAN tagging—Single tagging with normalized to bridge domain tag at ingress • Clearing all MAC address information • Global MAC limit • Global source MAC aging time • MAC moves • LACP and LLDP • Disabling MAC learning at global and interface level

Table 2: Features Supported on PTX10K-LC1301-36DD line card for PTX10008 routers *(Continued)*

Feature	Description
	<ul style="list-style-type: none"> • Native VLAN ID for Layer 2 logical interfaces • Single VLAN-tagged Layer 2 logical interfaces • Interface statistics <p>NOTE: The show ethernet-switching statistics command and child logical interface statistics for aggregated Ethernet are not supported.</p> • Flexible Ethernet services <p>NOTE: Enterprise-style Layer 2 logical interfaces aren't allowed under the flexible-ethernet-services encapsulation.</p> • Virtual switch • Persistent MAC learning (sticky MAC) • Service provider bridging: <ul style="list-style-type: none"> • Multiple logical interfaces on the same physical interface that are part of the same bridge domain • Ethernet bridge encapsulation <p>[See Layer 2 Bridging, Address Learning, and Forwarding User Guide.]</p> • Support for IRB-Supported items for IRB include: <ul style="list-style-type: none"> • All Layer 2 protocols already supported on the router Layer 3 protocols: BGP, IGMP, IS-IS, OSPF, PIM, and RIP Per-IRB logical interface MAC and statistics IRB Layer 3 multicast support with flooding only

Table 2: Features Supported on PTX10K-LC1301-36DD line card for PTX10008 routers *(Continued)*

Feature	Description
	<p>Address family support for IPv4 and IPv6, and support for IPv4 MTUs and IPv6 MTUs with different MTU values IRB interface in VRF routing instances Directed subnet broadcast support with IRB.</p> <p>[See Integrated Routing and Bridging.]</p> <ul style="list-style-type: none"> • Support for interface MAC limit action. You can specify the action (drop, drop and log, log, or shut down) that Junos OS Evolved takes when packets with new source MAC addresses are received after the MAC address limit is reached. <p>[See Configuring MAC Limiting and packet-action.]</p>

Table 2: Features Supported on PTX10K-LC1301-36DD line card for PTX10008 routers (Continued)

Feature	Description
Layer 3 Features	<ul style="list-style-type: none"> Support for 256-way ECMP. You can configure a maximum of 256 equal-cost multipath (ECMP) next hops for external BGP (EBGP) peers. This feature increases the number of direct BGP peer connections, which improves latency and optimizes data flow. However, we support 128 ECMP next hops for MPLS routes. Note that we do not support consistent load balancing (consistent hashing) for IPv4 or IPv6 with this feature. [See Understanding BGP Multipath.] Support for the following Layer 3 forwarding features for IPv4, IPv6, MPLS, LAG, ECMP, MTU checks, ICMP, OSPF, IS-IS, ARP, NDP, BGP, BFD, LACP, LDP, RSVP, LLDP, VRF-lite, TTL expiry, IP options, IP fragmentation, DDoS BFD support, including: <ul style="list-style-type: none"> Distributed BFD and BFD-triggered local repair (BFD authentication is not supported.) Independent micro BFD sessions enabled on a per-member link basis for a LAG bundle Inline BFD [See Understanding BFD.] BGP flowspec signaling support. BGP flow specification. BGP can carry flow-specification network layer reachability information (NLRI) messages on PTX10008 devices with LC1201, LC1202 and LC1301 line cards.. Propagating firewall filter information as part of BGP enables you to propagate firewall filters against denial-of-service (DOS) attacks dynamically across autonomous systems. The following match conditions are not supported:

Table 2: Features Supported on PTX10K-LC1301-36DD line card for PTX10008 routers *(Continued)*

Feature	Description
	<ul style="list-style-type: none"> • ICMP codes alone [inet/inet6] • Source/destination prefix with offset for inet6 • Flow label for inet6 fragment [for inet6] <p>Junos OS Evolved running on this router doesn't support the traffic marking action. To configure flow routes statically, configure the match conditions and actions at the [edit routing-options] hierarchy level.</p>
MACsec	<p>Media Access Control Security (MACsec) is supported on physical interfaces.</p> <p>[See Understanding Media Access control Security (MACsec).]</p>
	<p>Support for Media Access Control Security (MACsec) bounded delay protection.</p> <p>[See Configuring Bounded Delay Protection.]</p>
Managing Devices	<p>Support for additional RPCs for the gNOI certificate management (cert) service. Junos OS Evolved supports the following gRPC Network Operations Interface (gNOI) cert service RPCs:</p> <ul style="list-style-type: none"> • CanGenerateCSR() —Query if the target device can generate a certificate signing request (CSR) with the specified key type, key size, and certificate type. • RevokeCertificates()—Revoke certificates on the target device. <p>[See gNOI Certificate Management (Cert) Service .]</p>

Table 2: Features Supported on PTX10K-LC1301-36DD line card for PTX10008 routers *(Continued)*

Feature	Description
MPLS	<ul style="list-style-type: none"> • We support the following MPLS features: <ul style="list-style-type: none"> • Support for MPLS FRR—MPLS fast reroute (FRR) provides faster convergence time (less than 50 milliseconds) for RSVP tunnels. The Routing Engine creates backup paths and the Packet Forwarding Engine installs the backup-path labels and next hops. [See Fast Reroute Overview.] • Support for 256-way ECMP. You can configure a maximum of 256 equal-cost multipath (ECMP) next hops for external BGP (EBGP) peers. This feature increases the number of direct BGP peer connections, which improves latency and optimizes data flow. However, we support 128 ECMP next hops for MPLS routes. Note that we do not support consistent load balancing (consistent hashing) for IPv4 or IPv6 with this feature. [See Understanding BGP Multipath.] • Support for MPLS features,including: <ul style="list-style-type: none"> • CLI support for monitoring MPLS label usage • Inline MPLS and IPv6 lookup for explicit null • 32,000 transit LSPs • Explicit null support for MPLS LSPs • MPLS Label Block Configuration • MPLS over untagged Layer 3 interfaces

Table 2: Features Supported on PTX10K-LC1301-36DD line card for PTX10008 routers *(Continued)*

Feature	Description
	<ul style="list-style-type: none"> • MPLS OAM - LSP ping • JTI: OCST: MPLS operational state streaming (v2.2.0) • 2000 ingress LSP support • 2000 egress LSP support • Entropy label support • MPLS: JTI: Junos telemetry interface MPLS self-ping, TE++, and misc augmentation • LDP, including: <ul style="list-style-type: none"> • Configurable label withdraw delay • Egress policy • Explicit null • Graceful restart signaling • IGP synchronization • Ingress policy • IPv6 for LDP transport session • Strict targeted hellos • Track IGP metric • Tunneling (LDP over RSVP) • RSVP++ • RSVP-TE, including:

Table 2: Features Supported on PTX10K-LC1301-36DD line card for PTX10008 routers *(Continued)*

Feature	Description
	<ul style="list-style-type: none"> • Bypass LSP static configuration • Ingress LSP statistics in a file • RSVP-TE hitless-MBB with no artificial delays • 32,000 transit LSPs • Auto bandwidth • Class-based forwarding (CBF) with 16 classes • CBF with next-hop resolution • Convergence and scalability • Graceful restart signaling • JTI interface statistics and LSP event export • LSP next-hop policy • LSP self-ping • MPLS fast reroute (FRR) • MTU signaling • Optimize adaptive teardown • Node/link protection • Refresh reduction • Soft preemption

Table 2: Features Supported on PTX10K-LC1301-36DD line card for PTX10008 routers (*Continued*)

Feature	Description
	<ul style="list-style-type: none"> • Shared Risk Link Group (SRLG) • Static LSPs with IPv4 nexthop, IPv6 next-hop, and IPv6 nexthop with next-table support for bypass • Traffic engineering, including: <ul style="list-style-type: none"> • TE++: Dynamic ingress LSP splitting • Traffic engineering extensions (OSPF-TE and ISIS-TE) • Traffic engineering options: bgp, bgp-igp, bgp-igp-both-ribs, and mpls-forwarding <p>[See MPLS Applications User Guide .]</p> <ul style="list-style-type: none"> • Segment routing support. You can configure the following Source Packet Routing in Networking (SPRING) or segment routing features on the router: <ul style="list-style-type: none"> • MPLS (segment routing using IS-IS): <ul style="list-style-type: none"> • Ping and traceroute for single IS-IS node or prefix segment • BGP Link State (BGP-LS): <ul style="list-style-type: none"> • Segment routing extensions for IS-IS • Segment routing extensions for OSPF • BGP:

Table 2: Features Supported on PTX10K-LC1301-36DD line card for PTX10008 routers (*Continued*)

Feature	Description
	<ul style="list-style-type: none"> • Binding segment identifier (SID) for segment routing-traffic engineering (SR-TE) • Binding SID for SR-TE [draft-previdi-idr-segment-routing-te-policy] • Programmable routing protocol process APIs for SR-TE policy provisioning • Static SR-TE policy with mandatory color specification • Static SR-TE policy without color specification • IS-IS: <ul style="list-style-type: none"> • Adjacency SID • Advertising maximum link bandwidth and administrative color without RSVP-TE configuration • Anycast and prefix SIDs • Configurable segment routing global block (SRGB) • Node and link SIDs • Segment Routing Mapping Server (SRMS) and client • Topology-independent loop-free alternate (TI-LFA):

Table 2: Features Supported on PTX10K-LC1301-36DD line card for PTX10008 routers *(Continued)*

Feature	Description
	<ul style="list-style-type: none"> • Link and node protection for IPv4 addressing (not required for IPv6 prefixes) • Link and node protection for IPv4 addressing (required for IPv6 prefixes) • Protection for SRMS prefixes • OSPF: <ul style="list-style-type: none"> • Advertising maximum-link bandwidth and administrative color without RSVP-TE configuration • Anycast SID • Configurable SRGB • Inter-area support • Node and link SID • Prefix SID • Segment Routing Mapping Server (SRMS) and client • Static adjacency SID • TI-LFA: <ul style="list-style-type: none"> • Link and node protection • Protection for SRMS prefixes

Table 2: Features Supported on PTX10K-LC1301-36DD line card for PTX10008 routers *(Continued)*

Feature	Description
	<ul style="list-style-type: none"> • MPLS ping and traceroute for single OSPF node or prefix segment • IGP adjacency SID hold time • Path Computation Element Protocol (PCEP) for segment routing LSPs • BGP IPv4 labeled-unicast resolution over: <ul style="list-style-type: none"> • BGP IPv4 SR-TE with IPv4 segment routing using IS-IS and OSPF • Non-colored IPv4 SR-TE with segment routing using IS-IS and OSPF • Static colored IPv4 SR-TE with segment routing using IS-IS and OSPF • BGP Layer 3 VPN over: <ul style="list-style-type: none"> • Colored SR-TE tunnels and IPv4 protocol next hops • Non-colored SR-TE tunnels and IPv4 protocol next hops • BGP-triggered dynamic SR-TE colored tunnels • Class-based forwarding and forwarding table policy LSP next-hop selection among non-colored SR-TE LSPs • First-hop label support for SID instead of an IP address

Table 2: Features Supported on PTX10K-LC1301-36DD line card for PTX10008 routers *(Continued)*

Feature	Description
	<ul style="list-style-type: none"> • Path specification using router IP addresses (segment routing segment list path ERO support using IP address as next hop and loose mode) • SR-TE color mode: <ul style="list-style-type: none"> • 00—Route resolution fallback to IGP path • 01—Route resolution fallback to color only null routes • Static LSPs with member-link next hops for aggregated Ethernet bundles (also known as adjacent SID per LAG bundle or aggregated Ethernet member link) <p>[See Understanding Source Packet Routing in Networking (SPRING).]</p> <ul style="list-style-type: none"> • Layer 2 VPN feature support includes: <ul style="list-style-type: none"> • Transport of Layer 2 frames over MPLS (LDP signaling) • Layer 2 VPNs over tunnels (BGP signaling) • Simple Ethernet and VLAN-based cross-connect (also known as connections) • Local and remote switching • Ethernet and VLAN CCC • Single-tagged CCC logical interfaces • Control word • Regular and aggregated Ethernet interfaces • Layer 2 protocol pass-through

Table 2: Features Supported on PTX10K-LC1301-36DD line card for PTX10008 routers *(Continued)*

Feature	Description
	<ul style="list-style-type: none"> • Layer 2 circuit backup interface and backup neighbor • Layer 2 circuit statistics and CoS • VCCV with type 2 and type 3 <p>[See Layer 2 VPNs and VPLS User Guide for Routing Devices and TCC Overview.]</p> <ul style="list-style-type: none"> • VLAN ID lists for Layer 2 Circuits. VLAN ID lists allow you to link multiple VLAN ID's to a single logical interface for Layer 2 traffic. <p>[See vlan-id-list (Ethernet VLAN Circuit), vlan-id-list, and Configuring VLAN Identifiers for VLANs and VPLS Routing Instances.]</p> <ul style="list-style-type: none"> • MPLS-based Layer 3 VPNs support includes: <ul style="list-style-type: none"> • MPLS over Layer 3 VLAN-tagged subinterfaces • Per-next-hop label allocation • Mapping of the label-switched interface (LSI) logical interface label to the VPN routing and forwarding (VRF) routing table using the vrf-table-label statement • ICMP tunneling and MPLS traceroute • Disabling time-to-live (TTL) decrementing using no-propagate-ttl <p>[See Layer 3 VPNs Feature Guide for Routing Devices.]</p> <ul style="list-style-type: none"> • Support for IP-over-IP encapsulation to facilitate IP overlay construction over an IP transport network. An IP network contains edge devices and core devices. To achieve higher scale and

Table 2: Features Supported on PTX10K-LC1301-36DD line card for PTX10008 routers *(Continued)*

Feature	Description
	<p>reliability among these devices, use an overlay encapsulation to logically isolate the core network from the external network that the edge devices interact with.</p> <p>Static configuration or a BGP protocol configuration is used to distribute routes and signal dynamic tunnels. The dynamic-tunnels configuration creates IP-over-IP encapsulation-only tunnels in the Packet Forwarding Engine.</p> <p>The following are not supported:</p> <ul style="list-style-type: none"> • Dynamic tunnel de-encapsulation operation • Next-hop-based statistics for dynamic tunnels • IP fragmentation at tunnel start point and path MTU discovery for IPv4/IPv6 <p>[See Next-Hop-Based Dynamic Tunneling Using IP-Over-IP Encapsulation .]</p> <ul style="list-style-type: none"> • Redistribution of IPv4 routes with IPv6 next hop into BGP. Devices can forward IPv4 traffic over an IPv6-only network, which generally cannot forward IPv4 traffic. <p>[See Understanding Redistribution of IPv4 Routes with IPv6 Next Hop into BGP .]</p> <ul style="list-style-type: none"> • Link delay advertisement- You can get the measurement of various performance metrics in IP networks, which helps to distribute network-performance information in a scalable fashion. <p>[See How to Enable Link Delay Measurement and Advertising in IS-IS .]</p>

Table 2: Features Supported on PTX10K-LC1301-36DD line card for PTX10008 routers *(Continued)*

Feature	Description
Multicast	<ul style="list-style-type: none"> • Support for multicast-only fast reroute (MoFRR) for both IPv4 and IPv6 traffic flows. MoFRR is supported for PIM sparse mode (SM) and sourcespecific multicast (SSM) modes only. Support does not extend to Multipoint LDP-based MoFRR. [See Understanding Multicast-Only Fast Reroute.] • Bidirectional Protocol Independent Multicast for multicast traffic. See pim-snooping • Support for RSVP-based and LDP-based point-to-multipoint (P2MP) LSPs with graceful restart. In addition, the router supports IP unicast traffic in a label-edge router (LER) role and both IP unicast and multicast traffic in a label-switching router (LSR) role. [See Point-to-Multipoint LSP Configuration] • Support for MPLS features P2MP ping and P2MP LSPs traceroute. MPLS ping and traceroute provide the mechanism to detect data-plane failure and isolate faults in the MPLS network. The traceroute or ping is initiated to validate LSP paths on P2MP. [See MPLS Applications User Guide.] • Optimized fast branch updates. The method of making fastbranch updates to a multicast replication tree has been refined. Now, any membership changes in the tree trigger fast makebefore- break (FMBB) re-optimization of the tree and ensure that there is no traffic loss. [See Multicast Shortest-Path Tree.]

Table 2: Features Supported on PTX10K-LC1301-36DD line card for PTX10008 routers *(Continued)*

Feature	Description
	<ul style="list-style-type: none"> • Multicast support for Next-Generation MVPN (NG-MVPN) including IR, RSVP-P2MP, and LDP-P2MP provider tunnel, inclusive and Selective PMSI tunnel, Rendezvous-point tree (RPT)-shortest-path tree (SPT) mode, turnaround provider edge (PE) device, RP mechanisms such as auto rendezvous point (RP), bootstrap router (BSR), and embedded RP. [See Multiprotocol BGP MVPNs Overview, Understanding Next-Generation MVPN Concepts, and Understanding Next-Generation MVPN Control Plane.] • Multicast support for Next-Generation MVPN (NG-MVPN) including IR, RSVP-P2MP, and LDP-P2MP provider tunnel, inclusive and Selective PMSI tunnel, Rendezvous-point tree (RPT)-shortest-path tree (SPT) mode, turnaround provider edge (PE) device, RP mechanisms such as auto rendezvous point (RP), bootstrap router (BSR), and embedded RP. [See Multiprotocol BGP MVPNs Overview, Understanding Next-Generation MVPN Concepts, and Understanding Next-Generation MVPN Control Plane.]

Table 2: Features Supported on PTX10K-LC1301-36DD line card for PTX10008 routers *(Continued)*

Feature	Description
	<ul style="list-style-type: none"> • MVPN BIER with MPLS encapsulation- Junos OS Evolved supports the Bit Index Explicit Replication (BIER) architecture to simplify control and forwarding planes by eliminating the need for multicast trees and per-flow states. With BGP-MVPN as an overlay, you can configure BIER-enabled provider tunnels for multicast VPNs. [See BIER Overview and bier.] • IS-IS as routing underlay for BIER. Junos OS Evolved supports the advertisement of BIER information of one or more BIER sub-domains using IS-IS as the IGP underlay. Key BIER information such as BFR IDs and BFR prefixes in each subdomain are flooded through the IS-IS domain to generate the BIER forwarding table. [See IS-IS Extension for BIER and bier-sub-domain (Protocols IS-IS).]

Table 2: Features Supported on PTX10K-LC1301-36DD line card for PTX10008 routers *(Continued)*

Feature	Description
Network Management and Monitoring	<ul style="list-style-type: none"> • Local and Remote Port mirroring: <ul style="list-style-type: none"> • Local port mirroring is used to copy the packet entering or leaving the system or port and send sampled packet through pre-designated port provided by configuration to remote devices/servers. Applications running on servers can analyze these packets and use the results based on the requirement. • Remote Port-Mirroring is used to send a sampled packet to remote destination provided by configuration. Packet will be encapsulated in a GRE header. Remote port mirroring will make use of the Flexible tunnel interface (FTI), to encapsulate and send the packets out of the box. This feature will also provide an option for configuring policer for the given instance, so that rate of sampling can be policed. • Port Mirror support for EVPN-VXLAN • Filter and mirror ingress and egress traffic on any network port to CPU- Junos devices support filtering and mirroring incoming and outgoing packets, sending those packets to the CPU, and saving them into a file. This feature, on-device packet capture, can help you with protocol and application analysis, debugging, troubleshooting, network forensics, audit trails, and network attack detection. On-device packet capture (or "self-mirroring") sends the sampled copy to a CPU and writes the copy into a packet capture (.pcap) file. The process does not require you to use any device connected to your network device. <p>[See On-Device Packet Capture.]</p>

Table 2: Features Supported on PTX10K-LC1301-36DD line card for PTX10008 routers *(Continued)*

Feature	Description
	<ul style="list-style-type: none"> • Support for the sFlow technology, which is a monitoring technology for high-speed switched or routed networks. The sFlow monitoring technology randomly samples network packets and sends the samples to a monitoring station. <p>[See Understanding How to Use sFlow Technology for Network Monitoring.]</p>
	<p>Support for additional RPCs for the gNOI certificate management (cert) service. Junos OS Evolved supports the following gRPC Network Operations Interface (gNOI) cert service RPCs:</p> <ul style="list-style-type: none"> • CanGenerateCSR() —Query if the target device can generate a certificate signing request (CSR) with the specified key type, key size, and certificate type. • RevokeCertificates()—Revoke certificates on the target device. <p>[See gNOI Certificate Management (Cert) Service .]</p>

Table 2: Features Supported on PTX10K-LC1301-36DD line card for PTX10008 routers *(Continued)*

Feature	Description
	<ul style="list-style-type: none"> • Up maintenance association end points (MEPs) in distributed periodic packet management (PPM) • Distributed Y.1731 on synthetic loss measurement (SLM), delay measurement (DM), and loss measurement (LM) • Down MEPs on bridges, circuit cross-connect (CCC) , and Ethernet VPN (EVPN) • Distributed session support for connectivity fault management (CFM) on aggregated Ethernet • Enhanced CFM mode • IPv4 (inet) support for Data Model (DM) and synthetic loss message (SLM) • Action profile for marking a link down, except for EVPN and bridge up MEP • LM colorless mode • DM and LM on aggregated Ethernet if all active child links are on the same Packet Forwarding Engine • Supported CFM protocol data units (PDUs), as follows: <ul style="list-style-type: none"> • Continuity check messages (CCM) • LBM • LBR • Link Trace Message (LTM) • Link Trace Reply (LTR) • Delay measurement message (DMM)

Table 2: Features Supported on PTX10K-LC1301-36DD line card for PTX10008 routers *(Continued)*

Feature	Description
	<ul style="list-style-type: none"> • Delay measurement reply (DMR) • LMM • LMR • Synthetic loss message (SLM) • Synthetic loss reply (SLR) • Enterprise and service provider configurations • VLAN normalization • VLAN transparency for CFM PDUs • CoS forwarding class (FC) and CoS packet loss priority (PLP) for CFM • CFM session on child physical interface in distributed mode • SNMP • Chassis ID or Send ID type, length, and value • Trunk mode • Maintenance association intermediate point (MIP)
Platform and Infrastructure	Support for SYNCE timing, SYNCE over LAG, and Timing SNMP and MIB (SYNCE)

Table 2: Features Supported on PTX10K-LC1301-36DD line card for PTX10008 routers *(Continued)*

Feature	Description
	<p>Platform resiliency support. PTX10008 routers with specific line cards support platform resiliency. Resiliency enables the router to handle failures and faults related to the hardware components such as line cards, switch fabric, control boards, fan trays, fan tray controllers, and power supply units. Fault handling includes detecting and logging the error, raising alarms, sending SNMP traps, providing indication about the error through LEDs, self-healing, and taking components out of service.</p> <p>[See show system errors active.]</p>

Table 2: Features Supported on PTX10K-LC1301-36DD line card for PTX10008 routers *(Continued)*

Feature	Description
Segment Routing	<ul style="list-style-type: none"> • Support for SRv6 network programming in IS-IS. Use this feature to configure segment routing in a core IPv6 network without an MPLS dataplane. • To enable SRv6 network programming in an IPv6 domain, include the <code>srv6</code> statement at the <code>[edit protocols isis sourcepacket- routing]</code> hierarchy level. • To advertise the Segment Routing Header (SRH) locator with a mapped flexible algorithm, include the <code>algorithm</code> statement at the <code>[edit protocols isis source-packet-routing srv6 locator]</code> hierarchy level. • To configure a topology-independent loop-free alternate backup path for SRv6 in an IS-IS network, include the <code>transitsrh-insert</code> statement at the <code>[edit protocols isis sourcepacket- routing srv6]</code> hierarchy level. <p>See How to Enable SRv6 Network Programming in IS-IS Networks.</p> <ul style="list-style-type: none"> • Support for SRv6 network programming and Layer 3 Services over SRv6 in BGP. You can configure BGP-based Layer 3 service over an SRv6 core. You can enable Layer 3 overlay services with BGP as the control plane and SRv6 as the data plane. SRv6 network programming provides flexibility to leverage segment routing without deploying MPLS. <p>[See Understanding SRv6 Network Programming and Layer 3 Services over SRv6 in BGP.]</p> <ul style="list-style-type: none"> • Operations, Administration and Management (OAM) ping support for segment routing with IPv6 (SRv6) network programming. You can

Table 2: Features Supported on PTX10K-LC1301-36DD line card for PTX10008 routers *(Continued)*

Feature	Description
	<p>perform an OAM ping operation for any SRv6 segment identifier (SID) whose behavior allows upper layer header processing for an applicable OAM payload. As segment routing with IPv6 data plane (SRv6) adds only the new type-4 routing extension header, you can use the existing ICMPv6-based ping mechanisms for an SRv6 network to provide OAM support for SRv6. Ping with O-Flag (segment header) is not supported.</p> <p>[See ITU-T Y.1731 Ethernet Service OAM Overview and How to Enable SRv6 Network Programming in IS-IS Networks.]</p> <ul style="list-style-type: none"> • Support for SRv6 traceroute. We support the traceroute mechanism for segment routing for IPv6 (SRv6) segment identifiers. You can use traceroute for both UDP and ICMP probes. By default, traceroute uses UDP probes. For ICMP probes, use the traceroute command with the probe-icmp option. <p>[See How to Enable SRv6 Network Programming in IS-IS Networks.]</p> <ul style="list-style-type: none"> • SRv6 support for static SR-TE policy. You can configure static segment routing-traffic engineering (SR-TE) tunnels over an SRv6 data plane. Use the following configuration commands to enable SRv6 support: <ul style="list-style-type: none"> • For an SR-TE policy: <code>set protocols source-packet-routing srv6</code> • For an SR-TE tunnel: <code>set protocols source-packet-routing source-routing-path lsp name srv6</code>

Table 2: Features Supported on PTX10K-LC1301-36DD line card for PTX10008 routers *(Continued)*

Feature	Description
	<ul style="list-style-type: none"> For an SR-TE segment list: set protocols source-packet-routing source-routing-path segment-list srv6 <p>[See Understanding SR-TE Policy for SRv6 Tunnel.]</p>
	<p>Support for SRv6 micro-SIDs or uSID. You can compress multiple SRv6 addresses into a single IPv6 address (micro-SID).</p> <p>[See Micro SID support in SRv6, micro-sid, and block.]</p>

Table 2: Features Supported on PTX10K-LC1301-36DD line card for PTX10008 routers *(Continued)*

Feature	Description
Services Applications	<ul style="list-style-type: none"> • Inline monitoring services support for packet mirroring with metadata. [See Inline Monitoring Services Configuration.] • Hardware-based IPFIX export for inline monitoring services support. [See Understand Inline Active Flow Monitoring.] • Juniper Resiliency Interface support. [See Juniper Resiliency Interface.] • HTTP and TCP probe types for RPM. You can configure the http-get, http-metadata-get, and tcp-ping probe types for real-time performance monitoring (RPM) probes. You must configure the offload-type none statement to be able to commit the configuration. [See probe-server, probe-type, and rpm.] • Inline active flow monitoring support, including support for egress sampling, for multiple BGP next-hop support, and for MPLS, MPLS-IPv4, and MPLS-IPv6 templates. [See Understand Inline Active Flow Monitoring.]
Software Installation and Upgrade	Support for Secure zero-touch provisioning (SZTP). [See Secure Zero Touch Provisioning .]
	Support for ZTP using WAN interfaces. [See See Zero Touch Provisioning .]
Additional feature support	Firewall filter support. [See Firewall filter support .]

Table 2: Features Supported on PTX10K-LC1301-36DD line card for PTX10008 routers (*Continued*)

Feature	Description
	<p>Policer and policer overhead interop support</p> <p>[See Routing Policies, Firewall Filters, and Traffic Policers User Guide.]</p>

Chassis

- **Managing FPC states and fabric reachability faults on routers (PTX10008)**—You can use the `set chassis fpc` command to manage the online and offline states of FPCs on PTX10008 routers with:
 - JNP10008-SF5 Switch Interface Board (SIB)
 - PTX10K-LC1201-36CD or PTX10K-LC1202-36MR line card

Use the `set chassis fabric event reachability-fault` command to detect fabric reachability faults and trigger connectivity restoration. To view link details within fabric planes, use the `extended` keyword in the `show chassis fabric fpcs` and `show chassis fabric sibs` commands. You can also identify partially enabled fabric planes by using the `degraded` keyword in the `show chassis fabric fpcs` command output.

[See [chassis-fabric-reachability-fault](#), [show chassis fabric fpcs](#), and [show chassis fabric sibs](#).]

Class of Service

- **HCoS interoperability support (PTX10008 with the PTX10K-LC1301-36DD line card)**—By default, PTX10008 routers boot with PTX10K-LC1301-36DD line cards in interop mode. This mode does not support hierarchical class of service (HCoS) configuration on the PTX10K-LC1301-36DD line card. To enable HCoS on this line card, run the `set chassis interoperability express5-enhanced` command. Commit the change and reboot the router. After the reboot, the PTX10008 with the PTX10K-LC1301-36DD line card supports HCoS configuration.

[See [Hierarchical Class of Service Overview](#).]

- **Per-queue accounting of ECN packets (PTX10002-36QDD)**—Counters on explicit congestion notification (ECN)-enabled queues increment when the queues experience congestion or receive packets that encountered congestion on another device. You can view these per-queue ECN accounting statistics using the `show interfaces queue` command.

PTX10002-36QDD routers support ECN counters only in non-hierarchical CoS (non-HCoS) mode. To enable non-HCoS mode on PTX10002-36QDD routers, run the `set class-of-service options hierarchical-scheduler-disable` command. Then commit the change and reboot the router.

[See [ECN Packets per Queue](#) and [show interfaces queue](#).]

Precision Time Protocol (PTP)

- **Support for timing and synchronization Timing (PTX10008)**—We support G.8273.2 and G.8275.1 precision time protocols (PTP) profiles over link aggregation group (LAG) on PTX10008 routers. Packet-based timing relies on time stamp packets inserted in the data stream. Time stamps are inserted at the master node where a stratum 1 traceable reference is available, and then extracted at the slave clock where the synchronized frequency or phase reference is needed. In PTP, only slave nodes that require precise frequency synchronization need to incorporate the timing extraction circuitry, and the rest of the packet network can remain asynchronous, which is a key advantage over physical layer timing methods (for example, SyncE) that need synchronous timing circuitry at every node. Packet-based timing can also transmit both frequency accuracy and phase information, which is essential in applications such as wireless networks (e.g., LTE, 5G - class-C, TSN for URLLC applications), while SyncE is only capable of transmitting frequency accuracy. The feature also support interoperability with the other existing PTX10008 line cards.

[See [PTP over Ethernet Overview](#) and [G.8275.1 Telecom Profile](#).]

What's Changed

IN THIS SECTION

- [General Routing | 89](#)
- [Junos XML API and Scripting | 90](#)

Learn about what changed in this release for PTX Series routers.

General Routing

- **Control Board offline delay for system stability (PTX10008)**—After initiating a node halt, you must wait 1 minute before doing Control Board (CB) offline. Attempting to offline the CB within this period will result in an error message. This delay helps maintain the stability and proper functioning of the system.

[See [request chassis cb](#).]

- Starting in Junos OS Evolved Release 24.4R2, you can set the `set protocols ptp delay-comp interface ifd-name transmit tx-comp-in-nsec receive rx-comp-in-nsec` command to compensate for external latencies for a given physical interface (IFD) on PTX10008 routers. You can use it to compensate for transceiver latencies, which are significantly higher in PAM4 optics, and other delays such as optics latency and cable asymmetry. The range of latency that can be compensated is from -1000ns to +1000ns. See "ptp", "delay-comp", and "Precision Time Protocol Delay Compensation"
- When you run the `request vmhost zeroize` command to zeroize a single Routing Engine on a dual Routing Engine device, the CLI incorrectly displays a message indicating that it will zeroize both Routing Engines.
- **SMAC accounting mismatch (PTX10002-36QDD, and PTX10008)** – Source MAC (SMAC) accounting over accounts the byte counter by including the L2 overhead in an IP packet. Both ingress and egress accounting for a SMAC learnt on any interface is affected. The packet accounting and the number of SMAC addresses learnt is correct.

[See [MAC address accounting for L3 interfaces and aggregated Ethernet interfaces.](#)]

Junos XML API and Scripting

- **Refreshing scripts from an HTTPS server requires a certificate (ACX Series and PTX Series, and QFX Series)**—When you refresh a local commit, event, op, SNMP, or Juniper Extension Toolkit (JET) script from an HTTPS server, you must specify the certificate (Root CA or self-signed) that the device uses to validate the server's certificate, thus ensuring that the server is authentic. In earlier releases, when you refresh scripts from an HTTPS server, the device does not perform certificate validation. Before you refresh a script using the `set refresh` or `set refresh-from` configuration mode command, first configure the `cert-file` statement under the hierarchy level where you configure the script. The certificate must be in Privacy-Enhanced Mail (PEM) format.

[See [cert-file](#).]

Known Limitations

IN THIS SECTION

- [General Routing | 91](#)

Learn about limitations in this release for PTX Series routers.

For the most complete and latest information about known Junos OS Evolved defects, use the Juniper Networks online [Junos Problem Report Search](#) application.

General Routing

- This is a transient log which sometimes is seen when LSI is recreated. This has no functional impact. It's generated because of additional dependency of LSI with BD. System takes care of cleaning the token for which this error is generated. This can be confirmed through VTY command `> show sandbox token <>`. [PR1834443](#)
- In case of PTX, continuous MAC move events of same MAC between two or more interfaces will take a worst case maximum of 2 to 3 seconds, as the TOE block in PTX waits for an ACK from host before it can move the same MAC again to a new interface. The delay is due to the fact that the host ACKs are processed by the TOE block in a two second timer thread. Also, in the BX chipset, there is an additional FIB cache cleanup logic delegated to host, which can add bit more delay in clearing the FIB cache entries in DLU block, to allow new events for the same MAC. Until then the TOE thread will not allow the same MAC to be moved. Due to the above said limitation, the control plane in PTX cannot record more than one MAC move event within the same second. So, to detect and record MAC move events, the below configuration is suggested. `set protocols l2-learning global-mac-move threshold-time 10 set routing-instances <ri-name> switch-options mac-move-limit 1 set routing-instances <ri-name> switch-options mac-move-limit packet-action log`. [PR1839324](#)
- This `hdr_crc_err` in FI (Fabric Input block) is due to CRC error corruption in header part of the cell that gone past beyond the FEC. This will result in cell drop. When FPC (LC1301) is starting up user might see `dp_X_fi_X_intr_pcs0_hdr_crc_err` in inactive system errors. This interrupt happens during the link training phase before the switching core logic input is enabled. So, this cell with `hdr_crc_err` is dropped and not processed any further. This is expected as the preparation of the link is done earlier, however this will not impact the system as FI block will not be enabled, when this interrupt is raised, during training. This note is applicable for LC1301 and SF5 SIB hardware combination. [PR1873313](#)
- If FPC is yanked out ungracefully `out_of_range_spry_indx` interrupts might continue to come. This will stop once FPC is online back again. [PR1875117](#)

Open Issues

IN THIS SECTION

- [Class of Service | 92](#)
- [General Routing | 92](#)
- [Junos Telemetry Interface | 96](#)
- [Interfaces and Chassis | 96](#)
- [Operation, Administration, and Maintenance | 96](#)
- [Routing Policy and Firewall Filters | 96](#)
- [Routing Protocols | 97](#)
- [Service Application | 97](#)

Learn about open issues in this release for PTX Series routers.

For the most complete and latest information about known Junos OS Evolved defects, use the Juniper Networks online [Junos Problem Report Search](#) application.

Class of Service

- Default FC names (Factory defaults) can't be redefined in Junos-EVO. Different/Custom FC names can be used as an alternative. This has no bearing on the functionality. [PR1827230](#)

General Routing

- When DHCP trace options are enabled, there is a possibility that jdhcpd could core. In general, traceoptions should be enabled only for debugging. They should be disabled once debugging is done. [PR1771121](#)
- On all Junos and Junos evolved platforms with telemetry enabled, if the streaming server and export profile for reporting-rate are not properly configured in the analytics settings, rebooting the FPC would prevent any of the interfaces from coming up. [PR1779722](#)

- On Junos Evolved PTX platforms, the log message "CFMMAN: Parse Error: CFM CCM pkt TLV parsing error" may appear when an FPC or PFE is restarted and comes online. This message indicates that a CFM Continuity Check Message (CCM) was truncated, leading to an error while parsing the TLV (Type-Length-Value) fields in the packet. The error is transient and typically affects only a small number (usually 1 or 2) of CCM packets received immediately after the FPC or PFE becomes operational. It has no functional impact on CFM sessions or overall network operations. CFM continues to function normally, and no persistent degradation is observed. This issue does not consistently affect any specific CFM session and occurs only during the brief initialisation period of the hardware component. [PR1810549](#)
- On Junos OS Evolved based platforms, while using ping, traceroute, or other utility that requires host name resolution, an error is raised indicating hostname resolution has failed. [PR1822994](#)
- RPC and CLI validation failed for `cli show ethernet-switching table`. [PR1825059](#)
- On all Junos OS Evolved platforms when recursively resolved routes are changed or deleted, route churn potentially leads to the rpd process crash. [PR1830588](#)
- On Junos OS Evolved PTX10003 platform the command `indirect-next-hop-change-acknowledgements` is required in the `junos-default` configuration. If the said command is missing, it will result in packet loss. [PR1836337](#)
- On Junos OS Evolved PTX platforms, when subinterface is disabled using command `set interfaces <name> unit disable`, packets are still getting forwarded since IFL state remains up in ASIC. As a workaround, instead of disabling the subinterface, it should be deactivated using command `deactivate interfaces <name> unit <>` so that the subinterface is removed and packet flow will be stopped. [PR1843667](#)
- When multiple SIBs are offlined in succession, at times it can result in continuous traffic drops. [PR1849563](#)
- On PTX EVPN MPLS-VXLAN Stitching DC-GW, vxlan traffic might select NH from `inet3` table, which will cause traffic loss. In order to avoid this, increase LDP preference to use `inet.0` table to resolve the NH for vxlan traffic. [PR1853669](#)
- On all Junos OS Evolved platforms, enabling the BGP RIB-Sharding causes the routing protocol daemon (rpd) leading to spike and remain at 100% CPU usage due to a background task (such as the Route Target/User Interface (RT/UI) delete job) entering into the continuous processing cycle and looping behaviour. [PR1854481](#)
- DNS resolution for traceroute does not work for a router using the `mgmt_vrf` with 23.4R2-EVO. [PR1858650](#)
- When two or more SIBs are offlined/restarted in quick succession, transient host loopback wedge major alarms can be seen. [PR1860468](#)

- SSH issue from the Routing Engine to the FPC causes SIB HA timeout error upon Routing Engine switchover. All the SIBs reset as a result of that. [PR1860970](#)
- An LSI IFL remains in RPD even after being deleted by the interface manager daemon. It is visible in show interface routing but not in show interfaces, indicating that RPD still holds the IFL despite its removal elsewhere. rpd-agent does not send a delete message to RPD due to a reference count issue. Another daemon?likely l2ald?still holds a reference to the IFL. rpd-agent only sends the delete once all references are cleared, which doesn't happen in this case. The fix is to send a **delete pending** message from rpd-agent to RPD. RPD will treat this as a delete and remove the IFL, ensuring consistency across the system. [PR1866522](#)
- On all Junos OS Evolved platforms, a failure in internal process communication causes the system to stop responding to the show system applications app ndp detail CLI command or prevent applications from start/stop/restart. This issue occurs when systemd becomes unresponsive to requests initiated by sysman. There is no impact to traffic forwarding. [PR1866988](#)
- Configure family inet6 for interfaces which are part of v6 over v4 hierarchies like follows: v6 Route (RTT_USER) -> Indirect(44168)-> Unilist(44160) -> v4 Unicast(44152). [PR1870118](#)
- On Junos OS Evolved PTX10001-36MR platform with PTP (Precision Time Protocol) configured, a synchronization issue occurs between the PTP FPGA (Field Programmable Gate Array) and the MAC (Media Access Control)/PHY (Physical Layer). This results in timing errors on the local device, which might also propagate to downstream devices. The issue typically arises after restarting the evo-aftmand-bt or evo-cda-bt processes, which impacts the socket connection between these processes and the timingd service. As a result, timingd is no longer able to communicate with these components as expected. [PR1878029](#)
- MACsec traffic can be impacted due to incorrect port mapping. When MACsec logical interface is configured with a custom EAPOL ethertype profile on dual VLAN tagged interfaces, traffic fails in one direction while the MACsec session appears up. This issue is observed during WAN MACsec use cases on PTX10002-36QDD and PTX10003-80C platforms. The issue does not occur when MACsec logical interface is disabled. [PR1879375](#)
- During link detraining sometimes cru_err_pg_psc interrupt may be present for a very brief time in SIB. It is not a problem if its seen during offline. But should not occur during stable state. [PR1880275](#)
- On Junos Evolved PTX platforms, when configuring a firewall policy, specifying family any, and matching on inner IP payload (IPv4 or IPv6), matching does not work on Multiprotocol Label Switching (MPLS) packets. [PR1882315](#)
- In Junos OS Evolved, ARP resolution requests are throttled on FPC per logical interface level that is if resolution request on a logical interface expires then a throttle timer is started on that logical interface and no other resolution request could be generated on that logical interface when throttle timer is running. In this issue RE netstack is sending packets to FPC with hint to resolution request for already resolved IP address and triggering throttle timer. So resolution request for second IP

address on same logical interface could not be generated for some time which is triggering phone-home application 10 seconds time out. [PR1883158](#)

- This issue is likely to occur when the interfaces are activated/deactivated/created/deleted. This could be due to a) Bulk change in interface configuration or b) Admin-initiated application restart via command `request system application node re0 restart app <application>` c) System triggered automatic application restart due to internal events. Note that this issue occurs due to very rare combination of events and would not be seen in most use cases. There is no service impact when the issue occurs, and router operations are unaffected. [PR1885455](#)
- This is a transient log which sometimes is seen when LSI is recreated. This has no functional impact. It's generated because of additional dependency of LSI with BD. System takes care of cleaning the token for which this error is generated. This can be confirmed through VTY command `> show sandbox token.` `<>` [PR1834443](#)
- In case of PTX, continuous MAC move events of same MAC between two or more interfaces will take a worst case maximum of 2 to 3 secs, as the TOE block in PTX waits for an ACK from host before it can move the same MAC again to a new interface. The delay is due to the fact that the host ACKs are processed by the TOE block in a two second timer thread. Also, in the BX chipset, there is an additional FIB cache cleanup logic delegated to host, which can add bit more delay in clearing the FIB cache entries in DLU block, to allow new events for the same MAC. Until then the TOE thread will not allow the same MAC to be moved. Due to the above said limitation, the control plane in PTX cannot record more than one MAC move event within the same second. So, to detect and record MAC move events, the below configuration is suggested. `set protocols l2-learning global-mac-move threshold-time 10 set routing-instances <ri-name> switch-options mac-move-limit 1 set routing-instances <ri-name> switch-options mac-move-limit packet-action log` [PR1839324](#)
- This `hdr_crc_err` in FI (Fabric Input block) is due to CRC error corruption in header part of the cell that gone past beyond the FEC. This will result in cell drop. When FPC (LC1301) is starting up user might see `dp_X_fi_X_intr_pcs0_hdr_crc_err` in inactive system errors. This interrupt happens during the link training phase before the switching core logic input is enabled. So, this cell with `hdr_crc_err` is dropped and not processed any further. This is expected as the preparation of the link is done earlier, however this will not impact the system as FI block will not be enabled, when this interrupt is raised, during training. This note is applicable for LC1301 and SF5 SIB hardware combination. [PR1873313](#)
- If FPC is yanked out ungracefully `out_of_range_spry_indx` interrupts may continue to come. This will stop once FPC is online back again. [PR1875117](#)
- `[fabric] [fabrictag]` : Junos OS Evolved PTX10008: some ccl is not fixed by AH, when GRES is initiated while AH is in progress. [PR1843391](#)

Junos Telemetry Interface

- With pre-gnmi telemetry (telemetrySubscribe) streaming, when the subscription is made with need_eos flag set to false, where initial sync is not requested, there is a possibility that counters with zeros are also will be sent atmost once. If collector is not interested in those zeros counter can ignore those data., as its streamed only once. This is not an issue if collector is requesting with need_eos set to true in the request as zeros counters are already being sent atleast once in this scenario. [PR1843391](#)

Interfaces and Chassis

- On PTX10003 systems, it is not allowed to configure ZR optics (400G) through CLI. [PR1851078](#)

Operation, Administration, and Maintenance

- On a PTX10016, and possibly PTX10008, the router shows fabric link OAM fault causing the system to not function properly. [PR1900242](#)

Routing Policy and Firewall Filters

- Multiple policies under same routing instance when applied on interfaces were not working correctly as this was not supported earlier. Now support has been added .[PR1873569](#)
- On all Junos OS Evolved platforms, when two policers with the same initial name(First 15 characters of rate estimator name) and term names are configured, since the rate estimator name (combination of filter term name and policer name) which gets truncated to 15 characters, the two policers start using the same rate estimator and it can lead to possible early drops by the policer, based on the current traffic rate of the two policers. [PR1896496](#)

Routing Protocols

- The RPD process crashes on all Junos and Junos OS Evolved platforms in a highly scaled scenario of more than 2000 BGP peers if the BGP sessions are un-configured/brought down abruptly. This leads to loss of routing information and will lead to loss of protocol traffic. [PR1756603](#)
- On all Junos and Junos Evolved platforms with dual Routing Engines (REs), Protocol Independent Multicast (PIM) neighborship is not be maintained on the backup Routing Engine after a ppmd-agent restart. This can lead to loss of PIM neighbor state on the backup RE. [PR1880262](#)

Service Application

- When a device is rebooted with PAA installed in 25.2R1 , PAA installation on reboot may fail due to "Not found default vrf" error. This can be resolved by deactivating and activating or freshly installing the PAA configuration. [PR1886928](#)

Resolved Issues

IN THIS SECTION

- [General Routing | 98](#)
- [Flow-based and Packet-based Processing | 100](#)
- [Forwarding and Sampling | 100](#)
- [Infrastructure | 100](#)
- [Interfaces and Chassis | 100](#)
- [Network Management and Monitoring | 101](#)
- [Platform and Infrastructure | 101](#)
- [Routing Policy and Firewall Filters | 101](#)
- [User Interface and Configuration | 101](#)

Learn about the issues fixed in this release for PTX Series routers.

For the most complete and latest information about known Junos OS Evolved defects, use the Juniper Networks online [Junos Problem Report Search](#) application.

General Routing

- The cfmman process crashes with high scaled CFM configuration. [PR1780805](#)
- USB Media installation shows up minor alarm **Host 0 Voltage Threshold Crossed**. [PR1799443](#)
- In high-scale, high-load environments, the l2ald process might experience hangs during Apstra polling. [PR1828741](#)
- The Netconf output for xml format shows ping-success tag under ping failure situation. [PR1835388](#)
- "bt_mtip_chpcs_hw_clear_stats: failed" error will be seen post rebooting the device. [PR1838394](#)
- IPv6 Neighbor Discovery Packets Punted to RE Instead of Transiting through Core Interface. [PR1842666](#)
- Core dumps are incomplete after unzip. [PR1843642](#)
- On rare occasions under load conditions after a switchover, the ehmd process on the standby RE might crash. [PR1843884](#)
- Traffic going over LDP or LDPoRSVP route matching the CBF is getting impacted when PTX Junos OS Evolved platform working as PHP router with CBF configuration. [PR1847169](#)
- Traffic loss observed over load-balanced ESI LAG towards Provide Edge router in an EVPN-MPLS path on Junos OS Evolved PTX Series platforms. [PR1849188](#)
- Extend the interfaces optics-options configuration of dp init max duration for 400G ZR-M-HP optical transceiver. [PR1849814](#)
- FLT alpha algorithm gracefully rollback support. [PR1853326](#)
- MACSec statistics will not show up in the show interfaces <intf-name> statistics detail command output. [PR1853676](#)
- [DCF14] [EVPN-VxLAN] After running a series of negative trigger tests on scale setup for 16 hours, traffic loss is seen in one IPv6 stream on ptx10001-36mr in CRB Spine and Border Router Role. [PR1854283](#)
- The evo-aftmand process crashes on PTX Junos OS Evolved platforms. [PR1855307](#)
- Chassis synchronization clock enters holdover state upon secondary BITS input failure. [PR1855958](#)

- Missing traffic statistics through telemetry on PTX Junos OS Evolved platforms with MPC10E, MPC11E, and LC9600 line cards. [PR1856528](#)
- Post configuration changes on an AE interface MPLS traffic is discarded for other interfaces/AE interface on a different FPC. [PR1856732](#)
- Extra link flap will be seen when the link fails for a short time on PTX10000 with LC1202. [PR1857490](#)
- Disabling the PIM interface underneath the edit protocols pim interfaces *intf-name* hierarchy might still show PIM as still being UP instead of DOWN. [PR1857699](#)
- The IPv6 firewall filter applied on loopback 0 is not processing NS and NA packets. [PR1859044](#)
- On Junos OS Evolved based platforms "Sysman.re" crash file might be observed in particular conditions. [PR1859095](#)
- EVPN next-hop installation for ESI over VTEP fails after remote device restart on PTX and QFX platforms. [PR1859302](#)
- PFH Interface Down After PFE Offline and Re-anchor. [PR1859387](#)
- SNMP walk failure due to missing OID after FCO/TPA delete compression. [PR1859621](#)
- PPPoE over EVPN-MPLS tunnel does not work. [PR1861208](#)
- Control plane is not properly managing the label 1048575 for MPLS traffic, leading to service impact. [PR1861803](#)
- NPU's (Network Processing Unit) KHT (Kernal Hash Table) utilization shows 100% utilization post config commit. [PR1862048](#)
- [Google 22.3X80-D47] Wedge detected after multiple, rapid PFE restarts. [PR1866487](#)
- IS-IS adjacency between CE devices is not established over Layer2 circuit. [PR1867003](#)
- Applying a Layer2 filter on interface on results in protocol flaps and traffic disruption on other interfaces on the same PFE. [PR1869773](#)
- PTX10002-36QDD showing incorrect Power Status. [PR1870153](#)
- Route installation for MPLS labels fails when an RSVP LSP goes down. [PR1874004](#)
- Rare assert with an Junos OS Evolved process. [PR1874151](#)
- Transient traffic loss during multicast route convergence scenarios. [PR1876781](#)
- Link flapping occurs on stable subinterfaces when using QDD400GZR optics if any one subinterface in the channelized group is down. [PR1878198](#)

- Log messages getting disappeared after upgrade. [PR1878365](#)
- Display issue is observed for command output `show forwarding-options port-mirroring self-mirror`. [PR1878786](#)
- MACsec traffic impact due to incorrect port mapping. [PR1879375](#)
- Rare evo-cda-bt crash in PTX10008 Junos OS Evolved with multiple FPCs when one FPC fails. [PR1879439](#)
- `sw.egnh.cfg_discard` on MAC-VRF EVPN Gateway when VXLAN VNI is not configured. [PR1890878](#)

Flow-based and Packet-based Processing

- PTX10000 Junos OS Evolved: JFLOW exported flow data `InputInt` is set to zero when redirecting to routing-instance and redirecting back to default instance. [PR1858721](#)

Forwarding and Sampling

- The update of the `parcel_dump` script to support the new Aegon linecard. [PR1851396](#)
- JNP10K-LC1301 running on ASAN image will go into fault state after restart. [PR1853920](#)

Infrastructure

- File Descriptor leak in `fibd` process leads to core files of different processes such as Jade, SSHd and Stunnel. [PR1860358](#)

Interfaces and Chassis

- Mixing EP and SP style configurations on AE bundle causes traffic loss and protocol session failure on Junos OS Evolved PTX Series platforms. [PR1856651](#)
- LACP session destroy time is not getting updated in PFE. [PR1859633](#)
- Transit multicast traffic is getting blackhole due to peer interface flap. [PR1867231](#)

- Coredump during LAG disable. [PR1867603](#)
- Disabling a single AE IFL in a MAC-VRF can bring the entire AE interface down. [PR1875917](#)
- Interface remains administratively down state, fails to recover after execution of CLI command `request interface bounce`. [PR1880635](#)

Network Management and Monitoring

- PTX10000 Junos OS Evolved, cold start SNMP trap is unexpectedly sent when doing primaryship switchover from RE1 to RE0, or backup RE reboot followed by primaryship switchover. [PR1875093](#)

Platform and Infrastructure

- Process `evo-aftmand-bt` crashes on PTX10000 Junos OS Evolved platforms when command `request chassis fpc slot <> pfe-instance <> restart` is executed. [PR1844523](#)

Routing Policy and Firewall Filters

- Family inet firewall should not allow IPV6 prefixes when referenced with prefix-list. [PR1846624](#)
- The `firewalld` process crashes post specific set of filter related modifications performed in single commit. [PR1875725](#)

User Interface and Configuration

- On Junos OS Evolved platforms, HTTPS download fails when HTTPS URL is present in the configuration. [PR1839955](#)

Junos OS Evolved Release Notes for QFX Series

IN THIS SECTION

- [What's New | 102](#)
- [What's Changed | 102](#)
- [Known Limitations | 104](#)
- [Open Issues | 104](#)
- [Resolved Issues | 106](#)

These release notes accompany Junos OS Evolved Release 24.4R2 for QFX5130-32CD, QFX5130-48C, QFX5130-48CM, QFX5130E-32CD, QFX5220-32CD, QFX5220-128C, QFX5230-64CD, QFX5240-64OD, QFX5240-QD, QFX5700, and QFX5700E switches. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

What's New

There are no new features or enhancements to existing features in this release for QFX Series switches.

What's Changed

IN THIS SECTION

- [EVPN | 103](#)
- [General Routing | 103](#)
- [Junos XML API and Scripting | 103](#)

Learn about what changed in this release for QFX Series switches.

EVPN

- **Duplicate MAC detection timeout (QFX5000 Series switches)**—The default setting for auto-recovery-time is 5 minutes on these platforms only.

[See [duplicate-mac-detection](#).]

General Routing

- When you run the `request vmhost zeroize` command to zeroize a single Routing Engine on a dual Routing Engine device, the CLI incorrectly displays a message indicating that it will zeroize both Routing Engines.

Junos XML API and Scripting

- **Refreshing scripts from an HTTPS server requires a certificate (ACX Series and PTX Series, and QFX Series)**—When you refresh a local commit, event, op, SNMP, or Juniper Extension Toolkit (JET) script from an HTTPS server, you must specify the certificate (Root CA or self-signed) that the device uses to validate the server's certificate, thus ensuring that the server is authentic. In earlier releases, when you refresh scripts from an HTTPS server, the device does not perform certificate validation. Before you refresh a script using the `set refresh` or `set refresh-from` configuration mode command, first configure the `cert-file` statement under the hierarchy level where you configure the script. The certificate must be in Privacy-Enhanced Mail (PEM) format.

[See [cert-file](#).]

- **Stale ui-state.db data in persistent NETCONF sessions post-mgd restart**—Existing NETCONF sessions might fetch stale data from ui-state.db after `mgd -N` restart. New sessions correctly map the refreshed database. Scripts must establish new sessions post-restart to access updated values. Functional configuration remains unaffected. Script failures monitoring "local-host" NETCONF sessions—Scripts might fail when including "local-host" NETCONF sessions in monitoring operations. Internal sessions are now excluded from tracking. Scripts must filter out "local-host" sessions. No impact to internal application functionality.

Known Limitations

IN THIS SECTION

- [General Routing | 104](#)

Learn about limitations in this release for the QFX Series switches.

For the most complete and latest information about known Junos OS Evolved defects, use the Juniper Networks online [Junos Problem Report Search](#) application.

General Routing

- On Junos Evolved TD4 platform (QFX5130-48CM), intermittent link flaps cause the hardware link scan to malfunction, resulting in incorrect high values in the Correction Field (CF) of Precision Time Protocol (PTP) packets, causing improper timestamping. This impacts system time inaccuracies across the network and the overall timing synchronization of the network until remediated.

Open Issues

IN THIS SECTION

- [EVPN | 105](#)
- [General Routing | 105](#)
- [Interfaces and Chassis | 105](#)

Learn about open issues in this release for QFX Series switches.

For the most complete and latest information about known Junos OS Evolved defects, use the Juniper Networks online [Junos Problem Report Search](#) application.

EVPN

- When duplicate-mac-detect feature is configured, if the mac moves from leaf to network in a VXLAN environment, the action discard does not take effect. The mac move is prevented. As an alternate, use the action shutdown port instead which is also one of the supported options. [PR1871034](#)

General Routing

- A missing authorization vulnerability in the internal virtual routing and forwarding (VRF) of Juniper Networks Junos OS Evolved allows a local, low-privileged user to gain root privileges, leading to a system compromise. Please refer to <https://supportportal.juniper.net/JSA100060> for more information. [PR1765490](#)
- On QFX5130/QFX5700 platforms, in Ethernet VPN-Virtual Extensible LAN (EVPN-VxLAN) scenario, the Explicit Congestion Notification (ECN) Congestion Experienced (CE) bit is not be set for ECN-capable traffic when there is congestion. Since the CE bit is not set, packets will be dropped. [PR1880166](#)
- USB disks with Junos OS Evolved images from 23.4R2-EVO onwards might not be detectable by Windows. They still have valid images, and can be used for Junos OS Evolved installs. The only issue is that new images cannot be installed on these USB disks because Windows no longer recognizes these USB drives. [PR1819846](#)
- On Junos OS Evolved QFX platforms having OSPFv3 (Open Shortest Path First version 3) authentication with IPsec (Internet Protocol Security) configured, OSPFv3 IPsec packets are not being sent for OSPF processing, as they are treated as unknown multicast packets. This causes OSPF neighborship issues, leading to traffic disruption. [PR1862778](#)

Interfaces and Chassis

- Link with the DAC (SFP56-50G-DAC-3M) comes up with 25G default speed configuration when switch is rebooted. Hence, When 50G speed config is applied , peer side sees the link flap. [PR1836697](#)
- Issue is not related to QFX5220 and not related to optics (QSFP56-DD-400GBASE-DR4) as mentioned in the PR synopsis and Description. We encounter this issue is happening on the vendor side on the QFX5700. Input Error and Framing are small in number it should not have significant impact on traffic.[PR1848109](#)

Resolved Issues

IN THIS SECTION

- [EVPN | 106](#)
- [General Routing | 106](#)

Learn about the issues fixed in this release for QFX Series routers.

For the most complete and latest information about known Junos OS Evolved defects, use the Juniper Networks online [Junos Problem Report Search](#) application.

EVPN

- Duplicate traffic occurs in an EVPN-VxLAN DCI configuration with translation VNI. [PR1853110](#)
- In an EVPN-VXLAN CRB environment, when performing traceroute from CE to Spine's Peer device, Spine's VGA does not return a reply. [PR1896299](#)

General Routing

- Junos OS Evolved: A low-privileged user can execute arbitrary Junos commands and modify the configuration, thereby compromising the system (CVE-2025-52954). [PR1765490](#)
- When a VXLAN encapsulated IP packet, or an IP packet with UDP port matching the VXLAN UDP port, is received on a trunk interface that does not have VXLAN configuration it is dropped. The Issue is not seen with untagged layer 3 interfaces. [PR1805922](#)
- In high-scale, high-load environments, the l2ald process might experience hangs during vendor polling. [PR1828741](#)
- Packets are incorrectly directed to an inappropriate filter and are lost due to TCAM exhaustion. [PR1840632](#)
- Packet Forwarding Engine restart and high CPU utilization for evo-pfemamd process in large-Scale VXLAN Fabrics. [PR1845230](#)

- VXLAN packets with inner VLAN tag are dropped in transit device. [PR1849807](#)
- Disabling the PIM interface underneath the edit protocols pim interfaces *intf-name* hierarchy might still show PIM as still being UP instead of DOWN. [PR1857699](#)
- ECN copy support from VXLAN header to inner header on type-5 decap tunnels. [PR1865671](#)
- Rare assert with an Junos OS Evolved process. [PR1874151](#)

Upgrade Your Junos OS Evolved Software

For products impacted, see [Feature Explorer](#).

Follow these steps to upgrade your Junos OS Evolved software:

1. Using a Web browser, navigate to the All Junos Platforms software download URL on the Juniper Networks webpage: <https://www.juniper.net/support/downloads/>
2. In the Find a Product box, enter the Junos OS platform for the software that you want to download.
3. Select Junos OS Evolved from the OS drop-down list.
4. Select the relevant release number from the Version drop-down list.
5. In the **Install Package** section, select the software package for the release.
6. Log in to the Juniper Networks authentication system using the username (generally your e-mail address) and password supplied by a Juniper Networks representative.
7. Review and accept the End User License Agreement.
8. Download the software to a local host.
9. Copy the software to the device or to your internal software distribution site.
10. Install the new package on the device.



NOTE: We recommend that you upgrade all software packages out of band using the console because in-band connections are lost during the upgrade process.

For more information about software installation and upgrade, see [Software Installation and Upgrade Overview \(Junos OS Evolved\)](#). For more information about EOL releases and to review a list of EOL releases, see <https://support.juniper.net/support/eol/software/junosevo/>.

Licensing

In 2020, Juniper Networks introduced a new software licensing model. The Juniper Flex Program comprises a framework, a set of policies, and various tools that help unify and thereby simplify the multiple product-driven licensing and packaging approaches that Juniper Networks has developed over the past several years.

The major components of the framework are:

- A focus on customer segments (enterprise, service provider, and cloud) and use cases for Juniper Networks hardware and software products.
- The introduction of a common three-tiered model (standard, advanced, and premium) for all Juniper Networks software products.
- The introduction of subscription licenses and subscription portability for all Juniper Networks products, including Junos OS and Contrail.

For information about the list of supported products, see [Juniper Flex Program](#).

Finding More Information

- **Feature Explorer**—Juniper Networks Feature Explorer helps you to explore software feature information to find the right software release and product for your network.

<https://apps.juniper.net/feature-explorer/>

- **PR Search Tool**—Keep track of the latest and additional information about Junos OS open defects and issues resolved.

<https://prsearch.juniper.net/InfoCenter/index?page=prsearch>

- **Hardware Compatibility Tool**—Determine optical interfaces and transceivers supported across all platforms.

<https://apps.juniper.net/hct/home>



NOTE: To obtain information about the components that are supported on the devices and the special compatibility guidelines with the release, see the Hardware Guide for the product.

- **Juniper Networks Compliance Advisor**—Review regulatory compliance information about [Common Criteria](#), [FIPS](#), [Homologation](#), [RoHS2](#), and [USGv6](#).

<https://pathfinder.juniper.net/compliance/>

Requesting Technical Support

IN THIS SECTION

- Self-Help Online Tools and Resources | 109
- Creating a Service Request with JTAC | 110

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active Juniper Care or Partner Support Services support contract, or are covered under warranty, and need post-sales technical support, you can access our tools and resources online or open a case with JTAC.

- **JTAC policies**—For a complete understanding of our JTAC procedures and policies, review the JTAC User Guide located at <https://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf>.
- **Product warranties**—For product warranty information, visit <https://www.juniper.net/support/warranty/>.
- **JTAC hours of operation**—The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

Self-Help Online Tools and Resources

For quick and easy problem resolution, Juniper Networks has designed an online self-service portal called the Customer Support Center (CSC) that provides you with the following features:

- Find CSC offerings: <https://www.juniper.net/customers/support/>
- Search for known bugs: <https://prsearch.juniper.net/>
- Find product documentation: <https://www.juniper.net/documentation/>

- Find solutions and answer questions using our Knowledge Base: <https://kb.juniper.net/>
- Download the latest versions of software and review release notes: <https://www.juniper.net/customers/csc/software/>
- Search technical bulletins for relevant hardware and software notifications: <https://kb.juniper.net/InfoCenter/>
- Join and participate in the Juniper Networks Community Forum: <https://www.juniper.net/company/communities/>

To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool: <https://entitlementsearch.juniper.net/entitlementsearch/>

Creating a Service Request with JTAC

You can create a service request with JTAC on the Web or by telephone.

- Visit <https://myjuniper.juniper.net/>
- Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).

For international or direct-dial options in countries without toll-free numbers, see <https://support.juniper.net/support/requesting-support/>.

Revision History

3 October 2025—Revision 5, Junos OS Evolved Release 24.4R2-S1

21 August 2025—Revision 4, Junos OS Evolved Release 24.4R2

6 August 2025—Revision 3, Junos OS Evolved Release 24.4R2

5 August 2025—Revision 2, Junos OS Evolved Release 24.4R2

25 July 2025—Revision 1, Junos OS Evolved Release 24.4R2

Juniper Networks, the Juniper Networks logo, Juniper, and Junos are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered marks, or registered service marks are the property of their respective owners. Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice. Copyright © 2025 Juniper Networks, Inc. All rights reserved.